大学におけるアクセスマネジメントに関する研究(Dissertation_全文)

AUTHOR(S):

清水, さや子

大学におけるアクセスマネジメントに関する研究

Studies on Access Management in Universities

清水　さや子

2018 年 9 月

概要

情報処理技術の発展により，社会的に様々な仕組みがオンライン化されている．大学などの教育研究機関においても，業務や教育・研究などの様々な活動がオンライン化され，組織において情報サービスは必要不可欠なものになっている．

大学などの教育研究機関には，学生や教職員だけでなく，その他の様々な身分の人が様々な期間在籍し，様々なサービスを身分や所属に応じて利用する．大学に在籍する人や大学で提供される情報サービスは，中央で一元管理されているのではなく，それぞれの部局などで個別に管理されている場合が多い．また，情報サービスを利用するのに用いられる情報機器も，大学の備品と個人所有のものが混在し，多くは研究室などの単位でそれぞれ管理されているという特徴がある．そのため，大学などの組織では，中央の管理者が一元的に利用者や情報システム，情報サービスに対するアクセスマネジメントを行うことが難しい．

そこで，本研究では，大学のような組織において情報サービスを提供する際に，分散的に管理されている実態に合わせて効率よくアクセスマネジメントできる仕組みについて検討した．本研究では，組織の中央のシステム管理者，部局などの各サービスや利用者の管理者，研究室などにおける情報システムの管理者などの各管理者の観点より，分散して管理されている利用者，情報システム，情報サービスのそれぞれに対するアクセスマネジメントにおいて，分散して管理されている実情と合わせ，各管理者がそれぞれ分散的に効率的に，かつ安全性を確保しつつ管理が行えることを目指す．具体的に，利用者については，一時的に利用する人の扱いの課題を解決する仕組みを提案する．情報サービスについては，利用者と情報システムを組み合わせて提供されるものであると捉え，その組み合わせを利用者の属性を用いて管理するグループ管理の課題を解決する仕組みを提案する．情報システムについては，キャンパスネットワークとそれに接続される端末機器を管理する際の課題を解決する仕組みを提案する．これらについては，それぞれの仕組みの検討，実装，試験稼働，評価を行った．

その結果，大学などの組織において，各情報サービスを提供する際に，実情と合わせて分散的に管理できるようになり，中央のシステム管理者や各情報サービスの管理者などの管理の負担が軽減され，管理運用コストの低減につながった．今後大学における情報サービスは益々増加することが予想されるが，本研究で提案する概念や仕組みを取り入れるこ

とで，各組織における利用者，情報システム，情報サービスの管理運用コストの低減につながることが期待できる．

Abstract

Along with the development of information processing technology, various social mechanisms have been made online. In academic organizations like universities, various activities such as administrative work, education and research are brought online. Information services have become indispensable in academic organizations.

At an academic organization, not only students, faculty members and staffs who officially belong to the organization, but also persons in various other statuses are enrolled for various periods and use various information services according to one's status and affiliation. Information services provided and people enrolled in a university are not centrally managed in the center, but are managed individually by each department or section in many cases. In addition, it is characteristic that information terminals used for accessing information services include university owned equipment and personal belongings both, and most of them are managed in small units such as laboratories. Thus, it is difficult for a central administrator in such an academic organization to perform centralized access management of users, information systems, and information services.

In this research, we have examined mechanisms that can perform access management of information services in academic organizations efficiently according to decentralized management of users and information systems. From each viewpoint of a system administrator in the center of an organization, an administrator of services and users managed in a department, and an administrator of information systems in a laboratories, we aim for each administrator to make access management of users, information systems, and information services that are managed in a distributed manner, efficient and safe. With regard to management of users, we propose a mechanism to solve the problem of handling temporary users. With considering that information services are provided by combining users and information systems, we propose a mechanism to solve the problem of group management combining a user to a system using attributes of the user. With regard to management of information systems, we propose a mechanism to solve problems in managing terminal devices connected to the campus network of an academic organization. We have developed, have implemented, have tested and have evaluated each mechanism.

Using the proposed mechanisms, it becomes possible to manage information services in an organization such as a university distributedly according to actual circumstances. The burden of administrators at the central system and at each information service is reduced, and the operation

cost of the systems is as well. The use of information services in universities will continue to expand in the future. The concepts and mechanisms proposed in this research will hopefully reduce the cost in management of users, information systems, and information services in each organization.

目次

図目次

表目次

第1章　緒論

1.1 研究背景

社会的に様々な仕組みがオンライン化され, 情報通信技術は必要不可欠なものになっている[1][2]．オンライン化されたサービスを管理する際には，ユーザの情報やアクセスできるサービスをコントロールするいわゆるアクセスマネジメントが必要になる[3][4][5][6][7]. アクセスマネジメントは, アイデンティティについてのライフサイクルにおける管理と各リソースへのアクセス制御を行うアクセス管理から成る．

アクセスマネジメントは，従来は単一のリソースごとに各 SP（Service Provider）のサービス提供者が，それぞれ ID 管理を行っていた．情報システムの増加に伴い，統合認証基盤が整備され，組織の中で ID 管理を中央で集約し，IdP（Identity Provider）と SP を分離する（以下，統合認証モデルとよぶ）ようになった．一般的な統合認証モデルでは，中央で一元的に利用者の ID や属性などの情報や連携するサービスに対する権限などの管理を行い，クレデンシャル情報の管理やプロビジョニングなどが行われる．ゲストユーザなどの例外的な利用に対する制御なども行われる[8][9]．また，組織外が管理するサービスの利用に際しては, ID 管理を行う主体である IdP とサービスを提供する主体である SP を分離し，組織をまたがったサービス連携（以下，Federated ID Management モデルとよぶ）が進められつつある．Federated ID Management モデルでは，個人情報保護の観点から匿名性の維持などが課題とされている．

大学などの教育研究機関においても，業務や教育・研究などの様々な活動がオンライン化され，情報通信技術は必要不可欠なものになっており[10][11]，統合認証基盤の整備による ID の統合化が進められている．しかし，大学などの教育機関では，様々な種類の利用者が様々な期間存在し, 利用者に対する管理体制も利用者の身分や所属により異なるなど複雑であることより，中央で全利用者の一元管理は難しい．また，一つの組織の中でも提供されるサービスは多数あり, それらは中央だけでなく様々な部局等で分散的に管理されているため，中央で一元管理することが難しい．さらに，情報システムの管理などは研究室などの小単位で個別に管理が行われることより，中央で一元管理することが難しい．これらより，大学などの組織では，一般的な統合認証モデルのように，アクセスマネジメントを中央で一元的に行うことが難しい．一方，様々な組織において，所属組織を越えた組織とのサービスの共有が進められていることより，大学などの組織においても Federated ID Management モデルが進められつつある（図 1-1）．

大学などの教育研究機関では，学生や教職員が在籍する以外に，様々な身分の人が様々

な期間在籍する．在籍者の管理は，学生は学務担当係，教職員は人事担当係，派遣契約者は契約担当係など身分ごとに異なり，かつ，それらがそれぞれ中央で一元管理されているのではなく，それぞれの部局でばらばらに管理されている場合が多い．それ以外にも，様々な身分や異なる所属の人などが存在するが，それらの情報は集約されていないことが多く，組織の全利用者を把握することが非常に難しいという特徴がある．また，大学などの組織では，様々なサービスが提供されており，利用者は身分や所属に応じて利用する．提供されるサービスは，全学向けのサービスの他に，学部・学科などで提供されるサービスがあり，身分・所属によって，利用できるサービスが異なる．これらの提供されるサービスは，中央で一元管理されるのではなく，部局ごとに個別に管理されている場合が多い[12][13]．さらに，予算や物品などの管理だけでなく，PC や居室内ネットワークや Web サーバやファイルサーバなど情報システムの管理は，研究室などの比較的小さな単位でそれぞれ独立して行われているという特徴もある．

このような利用者や情報システム，情報サービスなどの管理が，中央で一元的になされておらず，分散的にそれぞれ管理されている組織（以下，分散管理組織とよぶ）においては，組織の中央の管理者が単純に利用者や情報システム，情報サービスに対する一元的なアクセスマネジメントを行おうとすると管理者に非常に大きな負荷がかかるため非常に難しく，アクセスマネジメントは実態と合わせて分散的に行われることが求められる[9]．一方，大学などの分散管理組織では，類似内容のサービスが組織ごとに構築されていることや，利用者は所属する組織にとどまらず，共同研究や非常勤講師としての授業など組織間の行き来が多いことより所属が異なる組織において所属する組織とできる限り同等にサービスが利用できるよう，提供されるサービスを統一化し，組織を越えたサービスとして利用できることが求められる．これらより，新たに情報サービスを導入する際には，サービスの統一化を目指しつつ，すでに分散的に管理されている実態に合わせた効率よいアクセスマネジメントが求められる[3][5]．

これらの背景の元，本研究では，分散管理組織における利用者と情報システムに着目し，これらを組み合わせオンライン化して情報サービスとして提供する際のアクセスマネジメントにおいて，分散して管理されている実情と合わせ，それぞれの管理者が分散して管理できる統一的な枠組みの構築を目指す．その枠組みでは，安全性を担保しつつ運用に関するコストを最低限に抑えることを目標とする．

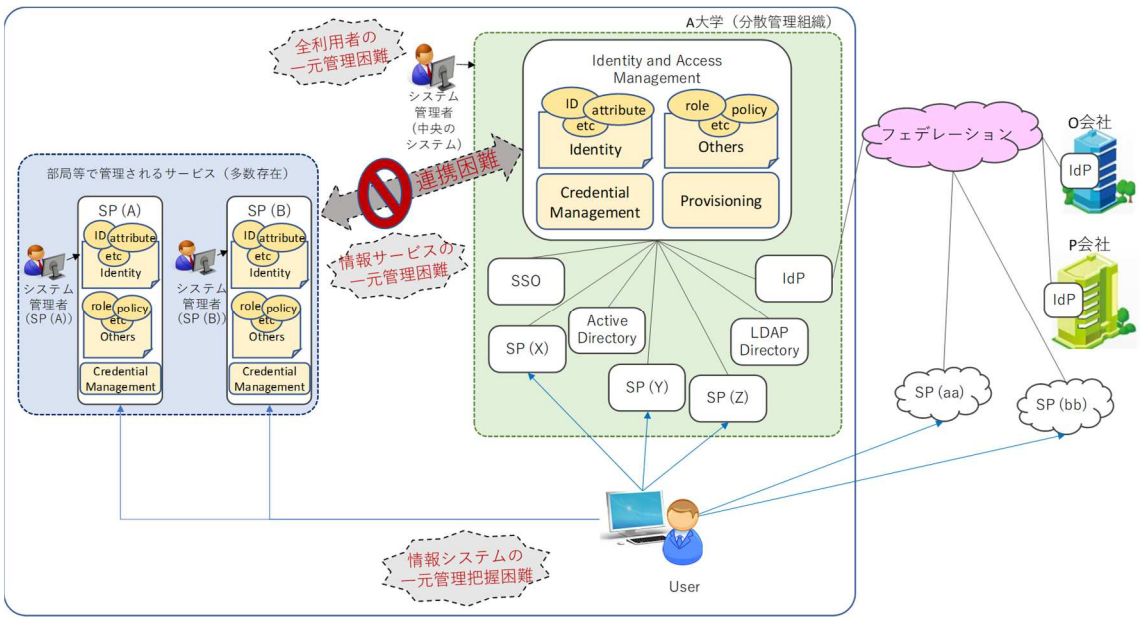

図 1 - 1　分散管理組織におけるアクセスマネジメント

1.2 研究の位置づけと研究方針

大学などの分散管理組織では，各組織において，組織を越えて互いに連携することで教育の質の保証や向上にもつながることより，大学間連携のサービスとして複数大学における e ラーニング教材の共有[14][15]や単位互換制度の導入[16][17]，産学との連携[18][19]などが検討され進められている．

情報サービスにおいても，類似的なサービスは，各組織で運用するより統一化もしくは共有化する仕組みが求められており，組織間連携に対する仕組みの検討が進んでいる[20][21][22][23][24]．国立情報学研究所が全国の大学等と連携して構築した学術認証フェデレーション（GakuNin）では，GakuNin に参加することで，互いに認証連携が行われ，所属する組織の ID を用いて，提供される SP を利用することが可能になる．GakuNin の参加機関向けに SP の提供を行うことも可能である[25]．

本研究においては，統合認証基盤が整備されている大学などの分散管理組織において，提供するサービスが組織間連携により組織を越えて利用できる統一化された仕組みになることを目指しつつ，そのための前段階として，利用者と情報システム，そしてそれらを組み合わせて情報サービスとして提供する際のアクセスマネジメントに対して，それぞれ個別課題を取り上げ，組織内向けの仕組みの検討を行った．個別課題では，利用者の個別課題として一時的に利用する人（以下，一時利用者とよぶ）向けの IC カード認証，情報

サービスの個別課題として統合 ID と属性を用いたグループ管理，情報システムの個別課題としてキャンパスネットワークと機器の管理の 3 つを取り上げ，それぞれの個別課題に対して，分散的に管理されている実態に合わせて各管理者がそれぞれ分散的に管理でき，かつ安全性を確保しつつコスト低減する仕組みを構築し（図 1-2），試験運用および評価を行った．

一時利用者向けの IC カード認証では，分散管理組織において，各サービスへのアクセス時に IC カードを用いた認証サービスを導入する際に，利用者の中で組織的に把握が難しく都度カードの発行が難しい一時利用者に対して，都度 IC カードを発行することなく，本人が日常的に利用している Suica などの IC カード（以下，一般カードと呼ぶ）を用いて各サービスを利用できる IC カード認証システムの仕組みを追求した．検討の仕組みでは，システム側や IC カード側に新たに情報を格納することなく，PIN コードを導くことができる仕組みを提案した．提案の仕組みを取り入れることにより，一時利用者に対するカード発行や管理に対する相対的なコスト削減を実現した．

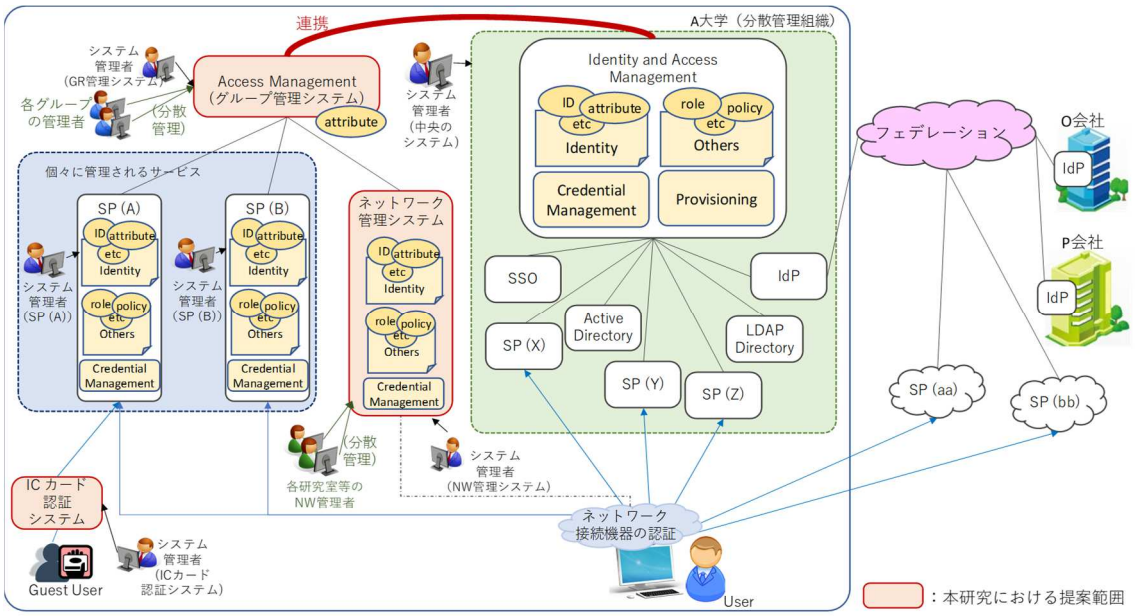

図 1 - 2　本研究の位置づけ

統合 ID と属性を用いたグループ管理では，組織内の部局などごとに管理されている利用者や情報システムを情報サービスとして提供する際に，グループを用いることで，各情報サービスでは個別にアクセス管理を行わなくてもよくなり，利用者はグループを介して情報システムにアクセスできるグループ管理の仕組みを検討した．グループは統合認証基

盤と連携して統合 ID と属性を用いて作成し，一般ユーザが参照権限を保持しつつ参照権限を越えたユーザをメンバとして自由に作成できる「一般グループ」と，業務で使用するためのグループに対して，グループ管理者を属性により指定し継続性を確保する「公式グループ」に分け，これらを使い分けることで，グループの管理およびグループ管理者の管理において，相対的なコストの削減を実現した．

キャンパスネットワークと機器の管理においては，研究室などの小単位でそれぞれ管理されている情報システムの管理において，統一的に管理するための仕組みの検討を行った．検討の仕組みでは，研究室などどの単位をグループとしグループに割り当てた IP アドレスの範囲内で接続機器の管理をすることによる管理コストの削減と，ネットワーク管理システムに登録した接続機器のみがネットワークに接続できる仕組みとした．登録した接続機器と IP アドレスを関連付けることでトラブル時の早期対魚などによる管理コストの削減を実現した．

一時利用者向け IC カード認証システムにおいては，一般カードを認証に使用する際，カード内情報を用いるだけでは安全性が低いことより，カード内情報とは別に利用者が入力する PIN コードなどの情報が用いられることが多い．しかし，PIN コードの情報は一般カードに格納することは非常に難しいため，IC カードを用いた認証システム側に PIN コード情報を格納するのが一般的である．しかし，そのようにすることで IC カードを用いた認証システムの管理者が一時利用者のカード情報や PIN コード情報を管理しなければならなくなり，全体的に把握されていない一時利用者に対してそれを行うことは非常に負担が高くなる．そこで，本研究では，システム側や IC カード側に情報を新たに格納することなく，PIN コードを導くことができる仕組みの検討し，システムの管理者の管理の負担を軽減し，相対的なコスト削減を実現するための仕組みを実装し，試験運用，評価を行った．

統合 ID と属性を用いたグループ管理システムにおいては，グループを用いた仕組みは，古くから検討されているが，大学などの分散管理されている組織向けに，統合認証基盤と連携して設計された仕組みとして米国では Grouper などが代表的である[26][27]．しかし，Grouper などの仕組みでは，グループの管理を柔軟かつ詳細にするほど，そのシステムの管理者やそのシステムの中でグループを管理する人の管理の負担が高くなるという課題があった．本研究では，統合認証基盤と連携したグループ管理の仕組みにおいて，Grouper などの既存の仕組みと実運用を照らし合わせ，グループに対する柔軟性や継続性などの課題において，システム管理者およびグループ管理者の管理の負担を軽減する仕組みの実装し，試験運用，評価を行った．

キャンパスネットワークと機器の管理システムでは, 研究室などの単位で管理されている IP アドレスや接続機器情報は，それぞれの研究室における教授などが主管理者となっているが, 実際には秘書や大学院生などが行っている場合が多い. これらの機器の管理に対して，ID の使いまわしなどを行うことなく，実務的に行っている人達が統合的に機器の管理が行えるよう上記で述べたグループ管理の仕組みと連携を行っている. また, 安全性向上のため, 機器の管理は厳格に行う必要があることより, 機器情報の一種である MAC アドレスを用いてネットワークの接続時に IP アドレスと関連付けて認証を行い，機器の監視を行うことで，正しい情報が登録されていない場合に通報する仕組みを取り入れる. これらの仕組みを実装し，試験運用，評価を行った.

本研究で実装した仕組みにおいては，大学などの分散管理組織において，1 つの組織内において分散管理されている実態と合わせて管理できる仕組みとして実装した. 本研究で提案する仕組みや概念は, 組織を越えた統一化したサービスとしても提供することが可能であり，組織間連携において，今後，他組織に提供できるようになることが期待できる.

1.3 全体構成

本論文の構成を述べる．本論文は 6 章で構成され，各章の内容は以下の通りである.

1 章では序論として, 本研究を行うに至った背景と目的および本研究の位置づけと研究方針，そして全体の構成について説明する.

2 章では，本研究における基本概念と従来研究について述べる．基本概念は，本研究の前提となる大学のような分散管理組織における特徴や統合認証基盤の概要について述べ, 分散管理組織で統合認証基盤を導入する際の課題や先行研究について述べる.

3 章では, 一時利用者向けの IC カード認証システムとして, 組織に IC カード認証を用いたサービスを導入する際，全体の把握およびカード発行が難しい一時利用者において, 一般カードを使いつつ, それぞれの部局などにおける部局のシステムの管理者が容易にサービスを提供できる仕組みの提案を行った. 一般カードを用いた認証サービスの既存の仕組みでは，カード内の読み取り可能な IDm（製造 ID）などの情報を用いて認証を行い, サービス管理者は認証に必要な情報を管理する必要があった. 本章で提案する仕組みでは, カード内情報を使用するだけでなく, セキュリティレベルに応じて, カード内情報と PIN コード, さらにカード内情報と ID・パスワードを組合せる. PIN コード認証を使う場合, カード側にもシステム側にも情報を格納せずに PIN コードを生成する PIN コード生成方式の提案，構築，試験運用と評価を行った．この仕組みを用いることで，各サービスの管

理者は IC カードや PIN コードの管理が不要となり，相対的なコスト削減を実現したことを報告する．

4 章では，統合 ID と連携した「グループ」機能を用いる際に，これまでのグループ管理の仕組みでは，グループの管理を柔軟かつ詳細にするほど，そのシステムを管理する人やグループの管理を行う人の負担が高くなるという課題があった．また，グループ管理者が不在となった場合のグループの継続性の確保が難しいという課題もあった．これらの課題が管理者間の権限移譲を効率的に行えるようにすることで解決できることを示し，それによりシステム管理者およびグループ管理者の管理の負担を軽減する仕組みを提案した．提案の仕組みでは，一般ユーザが自由に作成でき，参照権限を保持しつつ参照権限越えたユーザをメンバにできるグループを「一般グループ」と，業務などで使用するため継続性が求められる「公式グループ」に区別して扱い，グループ管理者の交代が自動的に行えるよう，グループ管理者を属性などで指定することを許す．これら二種類のグループを使い分け，システム管理者からグループ管理者，そしてグループ管理者から新グループ管理者へ，円滑にグループ管理の権限移譲を行うことで，相対的な管理コストの削減を実現したことを報告する．

5 章では，キャンパスネットワークへ接続する機器情報について，これまで研究室などの単位で個別に管理されていた IP アドレスや接続機器の情報に対して，組織内において統一的に管理できる仕組みの提案を行った．機器提案の仕組みでは，実態の管理体制と合わせて，研究室などの単位で接続機器の管理者らをグループとして管理できるよう，3 章で提案するグループ管理システムと連携し，グループごとに割当てた IP アドレスの範囲内で接続機器の管理を行えるようにした．また，安全性強化のため，キャンパスネットワークの接続時には MAC アドレスと IP アドレスを関連付けして認証し，機器の監視，通報する機能を取り入れた．これらの仕組みを MAC-IP 監視管理システムと呼び，2 段階に分けて試験運用を行った．試験運用の評価としては，接続機器の厳格な管理，不正に接続する機器を排除することによるトラブルの軽減，トラブル発生時に迅速に対応可能になるなど，相対的な運用コストの削減を行ったことを報告する．

6 章では，3 章から 5 章の各章で実装したサービスから得られた結論と，大学におけるアクセスマネジメントに関する今後の展望について述べる．

第2章　基本概念と従来研究

2.1 緒言

様々な仕組みのオンライン化により，業務の効率化，組織のグローバル化，サービスの多様化，スマートデバイス等の普及などが進んでいる．これらの中で情報サービスにおいては，かつては，サービスごとに異なる ID とパスワードが設定され，サービスごとに利用者情報が管理されていた．利用者にとってはサービスごとに異なる ID やパスワードを覚えなければならず，複数の ID とパスワードを覚えることは困難であることより，ID とパスワードを紙に記録したり，覚えやすい簡単なパスワードにするなど，管理が杜撰になっていた．サービスによっては，一つの ID を共通 ID として複数人で使いまわすようなこともあった．また，システム管理者にとっては，サービスが増えると管理の負担も増し，新規ユーザの登録漏れや，人事異動などによる属性の変更漏れや変更ミスなどが発生することもあった[28].

さらに，オンライン化されたサービスの管理においては，不正侵入による情報漏洩やデータ改ざん等のセキュリティインシデントにおける脅威があることより，適切なアクセスマネジメントを行うようにするなど，安全性に対する対策が必要とされていた[29].

これらの課題の解決のために，利用者の ID を統合化し，統合的に管理できる仕組みである統合認証基盤の整備が進められた[30][31]．統合認証基盤を整備することで，システム管理者はサービスごとに利用者情報を管理することが不要になり，利用者は一つの ID とパスワードで各サービスが利用可能になる．また，複数の Web サービスなどにおいては，一度パスワードを入力すれば複数サービスを同時に利用できるようになる SSO（Sigle Sign On）の仕組みの導入も進められた[32][33][34].

統合認証基盤の整備では，アイデンティティ管理と各サービスに対するアクセスマネジメントが重要になる．アイデンティティの管理においては，アイデンティティのライフサイクル管理，属性情報などの管理が必要になる．また，各サービスのアクセスマネジメントにおいては，連携するサービスに対する権限やポリシーなどの情報の管理が必要になる．

しかし，分散管理組織では，提供される情報サービスは，中央で管理するサービスだけでなく，部局や研究室などごとに管理するサービスも多く存在する．そのため，統合認証基盤を整備した際に，アクセスマネジメントできる情報サービスの範囲は中央で管理するサービスに限られている．部局等が管理するサービスにおいては，様々なサービスが様々な形で管理されているため非常に複雑であり，中央で統合認証を行う仕組み（以下，統合認証システムとよぶ）側では，アクセスしてきた情報の照合をすることはできるが，管理

部局の異なる各システムからの認可情報を中央で統一的に管理することは非常に難しく，行う場合は管理者に非常に負荷がかかるため行わないことが多い．そのため，部局等で管理する情報サービスのアクセスマネジメントはサービスごとに管理されるのが一般的となっている[9].

2.2 分散管理組織の特徴

大学のような組織では，利用者の情報やそれに関する ID，組織内で提供される情報サービス，情報システムなどは中央で一元管理されておらず，各部局などで分散的に管理されている．本研究では，このような分散管理組織を前提に，分散管理組織の特徴から導かれる情報サービス提供時の課題について，対応策を検討する．本節では，分散管理組織の特徴を述べる．

なお，大学などの組織で分散的な管理が行われていることは，米国でも同様であり，分散管理組織においてグループを分散的に管理する仕組みとして，Inetrnet2 プロジェクトによる Grouper などのサービスが開発されている．

2.2.1 利用者の管理

大学や大学共同利用機関などの分散管理組織は，学生や教職員が在籍する以外に，派遣等の契約職員や企業からの共同研究者など様々な身分の人が様々な期間在籍し，組織の様々なシステムを利用するという傾向がある．組織から給与が支給されている人，組織に対して学費として納めている人，給与は別に所属する組織から支給されつつ一緒に働いている人，学生として学費を納めつつ非常勤職員として契約して給与が支給されている人など，契約関係も多様である．また，組織内には，本務だけではなく兼務をしている人も多く存在する[35].

人の管理においては，学生は学務担当係，教職員は人事担当係，派遣契約者は契約担当係など身分ごとに管理部局が異なるなど分散的に管理されており，一元的に管理されていない場合が多い．また，複数の身分を有する場合，管理されているのは主の所属のみである場合も少なくない．一時利用者においては，管理部局が身分・所属などにより多部局に渡っていることが多く，それらの情報が集約されていないことが多いため，一時利用者を含む組織の全利用者を把握することが非常に難しい．また，分散管理組織の特徴は，一時利用者の在籍の管理が困難であるだけではなく，教職員と学生との仕切りが低いことや，元職員にも現職員と同等のサービスを提供しなければならない場合があること，非常勤講

師として雇用契約は結んでいるが，年 1 回だけ講義する可能性がある人が，正職員より多い数登録されている場合もあり，このような中では一時利用者を明確に線引きすることも困難である．大学という組織では非常に多くの一時利用者が存在し，その人数は正確には把握できていないが，1 年間における一時利用者数は，組織の全利用者の約 5 割以上と考えられる．

そこで，本研究における一時利用者は，ある程度在籍年数が決まった学生や教職員以外の短期間雇用の非常勤職員，共同研究員，派遣社員等とする．具体的には，組織の情報システムを利用するが，大学に来る期間が短いか期間が長くても来る回数が少ないため，アカウントや IC カードを発行するのが難しい人，あるいは，大学に正式な身分がないため，アカウントや IC カードを発行できない人とする．一時的に来構する訪問者や受験生は一時利用者には含まない．

2.2.2 情報サービスの管理

「サービス」は，人，物，情報など様々な要素を組み合わせることで提供される．大学などの組織においても，様々なサービスが様々な形で提供されている．提供されるサービスは全学向けのサービスの他に，学部や学科などの部局ごとに提供されるサービスがあり，身分・所属により利用できるサービスが異なる．利用可能なサービスは身分・所属ごとに異なるが，これらのサービスの全てが中央で一元管理されているのではなく，部局ごとに個別に管理されている場合も多い．これは，中央で管理されるサービスと部局ごとに管理されるサービスを連携する際の取り決めや手続きに時間を要することが多くあるためだけでなく，組織の特徴として縦割り運営が行われていることと，それに対して学部や学科ごとの特性を出すためでもある．情報サービスについても同様である．中央で管理されているサービスに，部局ごとに管理しているサービスを連携させる際，中央で管理するサービスの管理者と部局ごとのサービス管理者との取り決めや，アクセス時の制限等により，連携手続きに時間を要することが多くある．

組織内に多く存在する情報サービスの管理においては，統合認証基盤を整備することで，各情報サービスに対するユーザの ID を統合化することができるようになった．統合化された ID は，中央で管理し，各サービスを経由してアクセスしてきた ID に対する情報の照合をすることはできるが，中央では，管理部局の異なる各サービスに対して利用権を与えるいわゆる認可を行うことは難しく，行う場合は中央の管理者に非常に負荷がかかるため行わないことが多い．そのため，ID が統合化されても，部局などで管理されるサービ

スに対するアクセス制限の管理は，サービスごとに行われている場合が多い．

なお，学生の身分でありつつ非常勤職員などの身分も保有するなど 1 つの組織で複数の身分を有する場合，管理されているのは主の身分のみである場合が多い．このような場合，教職員に限定されたサービスや学生に限定されたサービスがあったとしても，主の身分である学生に限定されたサービスしか利用できないということが発生する．

2.2.3 情報システムの管理

大学などの組織では，人やサービス以外にも，予算，PC や実験器具などの備品，消耗品，薬品，部屋の入退室など管理が必要とされるものが多数存在する．これらの管理は，組織の中央で一元管理を行っているのではなく，学部や学科，研究室などの単位で管理が行われている．これは，学部や学科などで，独自性を出すため教育研究方針が異なることや，研究されている内容が研究室ごとに異なるため，これらを中央で一元的に管理することが非常に難しい．大学などの組織では，複数の学科で共同的に行う事業や，複数の研究室で共同研究が行われている場合，さらに，外部組織と共同で行う事業や研究がなされていることも多々あり，非常に複雑である．そのため，情報システムに関する管理は，学部や学科や研究室などの単位でそれぞれ行われている．管理する際の方法は統一されておらず，紙やエクセルなどの電子ファイル，専用のシステムを作っているなど，様々であった．

近年，情報技術の向上により，多くの組織において，物品や予算などの各資産管理や業務に対する管理方式が紙ベースから情報システムに変化しつつある[36][37]．最近では多くの研究がなされてきたことにより，各担当者が必要な範囲において情報を管理できる資産を管理するためのシステムが多く存在している．各資産管理システムへの認証は，統合認証基盤が整備されている組織では，別途中央で管理される統合認証基盤サーバと連携し，統合 ID を用いて認証する場合が多い[38][39][40] が，依然として，部局等で管理されるシステムのアクセス制限はシステムごとに行う必要がある．

2.3 統合認証基盤

統合認証基盤は，複数のサービスに対して ID の統合化を行い，複数のサービスを統合的に管理する仕組みであり，多くの組織において統合認証基盤の整備が進んでいる．統合認証基盤の整備が行われると，ユーザは一組の ID とパスワードで，メールシステムやポータルシステム，E-Learning システムなどの多くのサービスが，利用可能となる[30][32]．

統合認証基盤の整備では，中央に統合認証のためのシステム（以下，統合認証システム

とよぶ）が設置され，ユーザの ID・パスワードの他に，所属や身分など共通に定義される属性情報などユーザのアイデンティティ情報の管理が必要になり，これらは統合認証システム上で，一元的に管理される（図 2-1）．これらのアイデンティティ情報は，連携する複数のサービスへ影響することより，厳格な管理が求められる．

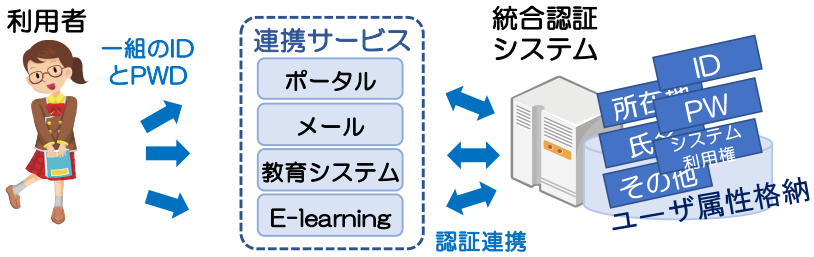

図 2 - 1　統合認証基盤導入における利用者のイメージ

2.3.1 認証と認可

認証（Authentication）とは，本人であることの確認である．本人を識別するための ID と，本人しか知り得えないパスワードの対などが一致すれば，本人であると見なされ，認証が成功する．ID とパスワードの組み合わせは，フィッシングやブルートフォース攻撃で破られる恐れがあり，一度破られると，後々に重大な被害を被る[41][42]恐れがあるため，さらなる認証の強化として，ID とパスワードの他に IC カードなどの複数の要素を用いてより確実な認証を行う多要素認証（二因子認証とよばれることもある）が用いられる場合もある[44][45][46].

認可（Authorization）とは，認証が成功した利用者に対して，各サービスの利用やリソースなどに対してアクセスを許可することである．各サービスやリソース側では，それぞれに設定されたアクセス制限のルールの元に，ユーザが認証に成功した後，アクセスを許可するか拒否するかを決定する．各サービスの認可を行うための手法として，ロールに対してアクセス制限を行う RBAC（Role-Based Access Control）や属性に対してアクセス制限を行う ABAC（Attribute-Based Access Control）が効率的なモデルとされており，効率化に関する検討が古くからなされている[47][48][49]．これらのモデルは，詳細な認可のルールが設定でき，認可ルールの変更時にも柔軟に対応できるが，組織が複雑になるほど管理負担が増し，開発や運用に関するコストが高くなるという課題もある．

2.3.2 統合認証システムを用いた認証と認可

統合認証システムでは，利用者のアイデンティティ情報の管理だけでなく，各サービスからの認証情報や，各サービスへのアクセス権限などの認可情報も管理することが可能である．統合認証システム上でアクセスマネジメントを行うことで，中央で管理されるサービスに対しては，利用者は一度パスワードを入力するだけで，複数の Web サービスが利用可能になる SSO の実現も可能である．

SSO を実現するためには，エージェント方式，リバースプロキシ方式，代理認証方式，フェデレーション方式などが用いられる．フェデレーション方式は，Office365 や G Suite などの海外のクラウドサービスが対対応しており，異なるドメイン間を，パスワードなどの情報を渡すことなくチケットと呼ばれる情報を受け渡しすることで，安全に認証されたユーザ情報を連携する．使えるプロトコルの標準化が進められており，「SAML（Security Assertion Markup Language）」や「OpenID Connect」が使われている[50][51].

SSO 導入により，利用者は 1 つのパスワードさえ覚えておけばよく利便性は高いが，そのパスワードが盗まれるとすべてのサービスに影響することより，セキュリティに対する脅威は増すため，ID とパスワードの他に IC カードなど多要素認証が推奨される．

2.3.3 アイデンティティ管理

アイデンティティ管理とは，サービスやリソースに対する，実体（エンティティ）の ID 情報などをライフサイクルに渡って管理する技術のことである．管理するエンティティの情報は ID の他に，パスワード，ユーザのアクセス権限，ユーザプロファイルなど多様な属性情報を管理する（図 2-2）．属性情報をオンラインで利用する際にも，利用者を本人であると認証すること，利用者の属性情報を交換すること，利用者の属性情報に基づいてアクセスを制御することなどがあげられる．そして，それぞれの目的に利用できる技術仕様が複数策定されている[3]．アイデンティティ情報を管理するためには，ライフサイクル全体に渡って「登録」・「更新」・「休止」・「抹消」のプロセスが適切に行われる必要がある．ライフサイクルの管理が適切に行われない場合，既に退職などによりアクセス権がなくなった人は抹消されるまで，在籍中にアクセス可能であったリソースにアクセスすることでき，情報漏洩やデータ改ざんにつながる恐れがあるため，プロセスの変更は即時に行われる必要である．また，異動などがあった場合に属性変更が行わなければ，旧所属でアクセス可能であったリソースにいつまでもアクセスすることができるが，新しい異動先で必要となるリソースにアクセスできず業務に支障をきたすこともある．特に，ID を統合化す

る際には，統合化された ID を認証に使用する全てのサービスに影響することより，これらのアイデンティティ管理は厳格に行われなければならない．

図 2 - 2　（例）A さんのアイデンティティ情報

2.3.4 分散管理組織におけるアイデンティティ管理の課題

分散管理組織には，学生でありつつ非常勤職員として採用されているなど複数の身分を有する人が多く存在する．統合認証基盤を導入した際に，中央で管理される属性は，全ユーザ共通であり，ユーザごとに異なるわけではない．そのため，中央で管理される情報は，本務として登録されている所属や身分のみが管理される場合が多い．そのため，連携するサービスの利用は，本務として登録されている所属や身分の属性に対して利用可能になる．原則的に，兼務などでアクセスを必要とするサービスへはアクセス不可となる．兼務の身分として連携サービスへのアクセスが必要な場合は，別の ID を登録するなどして対応している場合もある．

複数の身分を有する人は，実際は本務だけでなく，兼務やさらに詳細な単位で動くことも多い．例えば，G センター所属の O 教授は，J 研究科の教授職も兼務している場合を考える．共通で定義される所属属性は，G センターになり，兼務の所属である J 研究科に含まれない場合，J 研究科が提供する J サービスにおいて，所属属性が J 研究科となっている人のみアクセス可能と設定されていると，O 教授はそのサービスが利用できない．それだけだはなく，J サービスの管理者は，設定した所属属性に含まれるユーザの情報が分からないため，O 教授がアクセス不可であることも分からない場合もある．このような場合，中央の認証基盤で O 教授が J 研究科所属であるという ID を別途発行するか，J サービスの管理者が O 教授用に個別にアクセスできる ID を発行するか，O 教授が利用できないままにするなど，取られている手段は組織により様々である．

2.3.5 分散管理組織における認証認可の課題

大学などの分散管理組織では, 統合認証システムで認可の情報を管理できるサービスの範囲は中央で管理するサービスに限られている．部局等が管理するサービスにおいては, 様々なサービスが様々な形で管理されているため非常に複雑であり, 中央の統合認証システム側では, アクセスしてきた情報の照合をすることはできるが, 管理部局の異なる各システムからの認証に対しては, 中央で統一的に認可情報を管理することは非常に難しく, 行う場合は管理者に非常に負荷がかかるため行わないことが多い．そのため, サービスごとに管理されるのが一般的である[9][52].

統合認証基盤においては, 認証情報に関する統合化や管理の効率化に関する研究, またそれを使った組織間連携における認証の仕組みの効率化の研究が進められている[31][32][53]．部局等が管理するサービスを含めた認可情報に関する管理の効率化や組織間連携については十分な普及に至っておらず, 統合的かつ効率的に管理できる仕組みが求められている．

各サービスのアクセス制御を行う際, サービス側にアクセスを許可するユーザとアクセス範囲の設定が必要になる. 大学などの組織では, 部局等が管理するサービスにおいては, サービスごとにサービスの管理者がユーザリストを作成し管理するか, 認証サーバに格納されている属性を指定するなどにより行うのが一般的である．前者の場合, サービスの管理者の負担が大きく, 削除漏れや追加漏れが発生する可能性も高いため, 後者の設定をする場合が多い．しかし, 中央の認証サーバで管理される属性は, 組織内の共通フォーマットとして管理される ID やパスワードの他, 氏名や性別, メールアドレス, 所属などに限られる．成績情報などの詳細な情報は, 個々の部局のサーバで管理される場合が多い．そのため, 認証サーバに格納されている属性を指定するだけでは, 各サービスが必要とする詳細な認可の設定を行うことは難しい．そのため, 詳細な認可の設定を行う場合は, 個々に列挙するユーザリストと属性から導かれたユーザの集合を組み合わせる．

また, 各サービスで認可するユーザの集合は, 複数のサービスで内容が重複する場合が多いにも関わらず, 通常はサービスごとに管理されている．そのため, 提供するサービスの数が増えるほど, 各サービスの管理者の負担が大きくなり, 認可ユーザの登録, 削除漏れが発生する可能性が高くなり, 効率が悪い．そこで, 部局等が管理するサービスの認可するユーザの情報を統合的に管理できる仕組みが求められる. 部局等が管理するサービスの認可情報を「グループ」として管理している仕組みが存在する．詳細は 2.4 に記す.

2.3.6 フェデレーション

フェデレーションは，複数のインターネット上のユーザ認証の連携を行うことであり，分散管理組織においては，統合認証基盤の整備により組織内で統合化された ID を，ID 連携することで，共通のプロトコルを用いて海外のクラウドサービスや組織を越えた統一化されたサービスが利用可能になる．フェデレーションでは，SP 側にはパスワードを持たず，IdP からの認証結果によってアクセスが許可される．

学術の世界における組織間連携では，大学と産学による連携や，大学間においては単位互換ができる制度の設置や，交換留学制度などが行われている．産学の連携においては，米国や英国では様々な形態での産学連携が進展し，技術的の創出やその移転が活発に行われているが，それに比べると日本は本格的に進展している状況ではなかった[54][55]ため，近年，産学連携活動の促進に向けた検討も進められている[18][19].

情報技術を用いた大学間の連携としては，日本国内では，国立情報学研究所（NII）が行った全国共同認証基盤 UPKI の構築や[23][56]，全国の大学等と連携して学術認証フェデレーション「学認（GakuNin）」の構築が行われ，様々な研究がなされている[8][57][58][59]．GakuNin では，Shibolleth を用いて連携を行い，各組織はフェデレーションが定めた規程（ポリシー）を信頼しあうことで，相互に認証連携を実現することが可能となる．個人情報保護の観点から属性に対する匿名性の維持などが課題とされている[60][61]が，認証連携を実現すれば，所属する組織の ID とパスワードを用いることで，他組織や他社が提供するクラウドサービスなども利用可能になる．例えば，他大学の無線 LAN をいつも大学で使用している ID とパスワードで利用することができ，かつ自大学が契約している電子ジャーナルへシームレスにアクセスすることも可能となる[25].

欧州では，GÉANT(旧 TERENA)で開発された国際無線 LAN ローミング基盤である eduroam が， 業界標準の IEEE802.1X に基づいており，参加している組織は，国内外の訪問先機関の無線 LAN が利用できる．eduroam は，日本では eduroam JP サービスとして，国立情報学研究所が提供する国内外の大学等教育研究機関の間でキャンパス無線 LAN の相互利用を実現するために構築されている[62][63]．eduroam は 2018 年現在，国内では 225 機関(46 都道府県)，世界約 90 か国(地域)が参加する．

2.4 グループ管理

分散管理組織において，各サービスの認可するユーザの情報を統合的に管理するために，統合認証基盤と連携し，アクセス可能なユーザの集合を「グループ」として管理する仕組

みが存在する．「グループ」を用いて認証認可を行う場合，グループを管理する仕組みでグループの登録・管理を行い，そのグループを用いて各サービス側で，アクセスを許可するグループとそれに対するアクセス範囲の指定を行う．複数のサービスで認可情報が重複する場合，該当するグループを指定すればよく，サービスごとに認可情報を詳細に管理することは不要となる．

2.4.1 グループのライフサイクル

グループは，組織の編成など，必要に応じて作成される．グループの目的は様々であり，管理方法や作成，消滅時期などはグループごとに異なる．運用していくうちに，拡大や縮小を繰り返し，メンバ交代なども行われる．そして，何度も見直しが行われ，目的が達成されると解散，解体する[64]（図 2-3）． グループでは，打合せ，相談，メンバ確認などを行うことができる．

情報システムにおいても，グループは存在し，ファイルやスケジュールの共有（メンバ向け投稿），メーリングリストの利用，システムの利用権限の設定，メンバ確認などの用途で使われる．一つのグループが多くのグループウェアを使うことも多い[90]．そのため，それぞれのグループウェアで共有できるグループとして管理されることが望ましい．また，グループは，1 人につき 1 つのグループではなく，複数のグループに所属していることが多い．

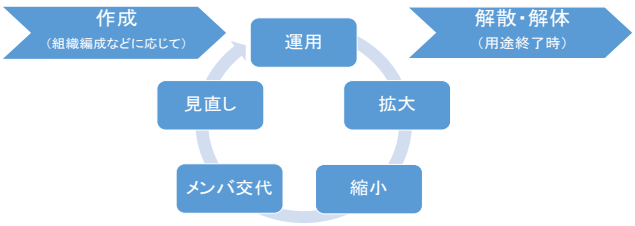

図 2 - 3　グループのライフサイクル

2.4.2 グループ管理とメンバ定義

組織内には様々なグループが存在する．グループは，グループごとに用途や規模が異なり，グループの作成時期やメンバの変更時期などもグループごとに異なる[65]．そのため，グループを中央で一括して管理することは，中央の管理者に非常に負荷がかかるため，グループごとに管理者を立て，分散的に管理することが求められる．

グループのメンバを定義する際，メンバとしたい人を列挙する方法が広く用いられてい

る．しかし，これはメンバを個々に管理することになり，グループ管理者の負荷が高くなるため，ユーザの属性などから条件式によりメンバが導かれる方法が望まれる．ユーザ属性の変更に合わせてメンバが更新される仕組みとすることで，グループ管理者の管理の負荷は非常に低くなる．さらに，作成済のグループに対する集合演算を用いてメンバを導く方法もある．この場合にも，作成済のグループのメンバの変更に合わせてメンバが更新されることで，グループ管理者の管理の負荷は非常に低くなる．

2.4.3 グループ管理の先行研究

グループを統合認証基盤と連携し，中央でグループ管理を行う仕組みの例としては，米国 INTERNET2 のプロジェクトで大学などの分散管理の環境のために設計された中央アクセス管理システムである Grouper，Exgen Networks 社の統合ディレクトリ管理を行うソフトである LDAP Manager [66]のオプション機能にあるグループ管理機能，国立情報学研究所で研究開発されている GakuNin に参加する組織において，所属組織を越えたメンバをグループとして管理できる GakuNin mAP[67]などがある．また，大学間連携の学術認証フェデレーション（GakuNin）においては，グループを属性として提供するための仕組みが提案されている[68][69][70].

Grouper などのこれまでのグループ管理の仕組みでは，システム管理者からグループ管理の権限を移譲された人がグループ管理者となり，グループやメンバを登録する．システム管理者がグループ管理の権限を移譲する際，グループ管理者ごとにユーザやユーザ属性に対する参照権限の設定を行う．グループ管理者に任命された人は，与えられた参照権限の範囲内において，グループの作成，メンバ管理などを行う．グループ管理者がメンバを登録する際，参照権限の範囲内のユーザリストや属性からメンバを選択し登録する．

LDAP Manager のグループ管理機能は，統合ディレクトリ管理を行うソフトである LDAP Manager のオプション機能である．システム管理者が必要に応じてグループ管理者を立て，グループ管理者はメンバを個々に列挙することでグループ管理を行う．ユーザ属性から導くことや既に作成されているグループを組み合せてグループを作成する際には，グループ管理者ではなくシステム管理者が行う．

GakuNin mAP は，学術認証フェデレーション（GakuNin）に参加する大学などの学術研究機関において，所属組織を越えたメンバをグループとして管理できる仕組みである．必要に応じてユーザがグループ管理者になり，メンバ管理を行う．メンバ登録は個々に列挙する形で行い，グループを階層化して管理できる．概念的には属性により導くことが可

能である．実際にメンバ登録の操作では，メンバにしたいユーザのメールアドレスを個々に登録する．プライバシー配慮のため，SP コネクタと呼ばれる各サービスとグループの間の接続管理の機能を用いており，SP コネクタに接続しなければ一切情報は流されない．

既存のグループ管理の仕組みでは，グループ管理者やメンバが限定的であり，グループの管理を柔軟かつ詳細にするほど，システム管理者やグループ管理者に対する管理の負担が大きくなるという課題がある．

グループ機能は，近年では，Facebook や Google などの Web サービスにおいても用いられており[71][72]，教育のツールとして用いられる場合もある[73][74]．これらは，ユーザが必要に応じてグループ管理者となり，個々にメンバ管理を行う．しかし，メンバの管理を行う場合，小規模なグループ管理にはよいが，大規模な組織などで使用するには管理者の負担が大きいため，ユーザ属性を用いることや既存のグループを組み合せてメンバを導くことが求められる．また，サービスごとに独自に管理されるため，メンバリストが重複する場合でも，サービスごとに管理する必要がある．

第3章　一時利用者向けの IC カード認証

3.1 緒言

統合認証システムや SSO システムの導入により，アカウントとパスワードの一元化が進みつつある. アカウントとパスワードの組み合わせはフィッシングやブルートフォース攻撃で破られる恐れがあり，一度破られると，後々に重大な被害を被る恐れがある．そのため，さらなる認証の強化のために IC カードが使われることが増えている．大学などの組織においても, 情報システムや入退館システムの利用のために認証システムが重要になり，IC カードをそれ単体ではなく身分証と一体化させて導入することが増えている[75][76]．しかし，大学などの組織で IC カードを導入する際，発行・管理する部局を巡って調整に多くの時間を要することや, 利用者の身分・属性によって管理部局が異なることより，利用者の全てではなく一部のユーザに対してのみ IC カードが導入されていることがある.

大学などの分散管理組織では, 一時利用者の管理部局が多部局に渡っていることが多く, 全体を把握することが非常に難しい. このような組織では, 一時利用者が着任する度に IC カードを発行し離任の度に回収することは難しい．一時利用者には，必要に応じていわゆる白カードの貸出しを行っている組織はあるが[77]，多くの組織では一時利用者にはカードを発行せず，一時利用者は IC カードを用いたシステムが利用できない状態であることが多い.

一般企業においても，業態によっては，部局ごとに契約している派遣社員や委託業務従事者，取引先社員等が在籍し，入れ替わりが激しいため，全体把握が困難となることがある．そのような組織で，IC カードが導入された場合も大学の一時利用者と同じ問題が発生することが考えられる.

本研究では，組織全体として IC カードを導入しているが一時利用者には発行していない組織，IC カードを導入していないが IC カードを使った認証システムの導入を検討している組織において，IC カードを用いた認証システムにおける一時利用者対応の管理運用の煩雑さやカード発行に関するコストを最低限に抑えるため，一時利用者には IC カードを発行せず，本人が日常利用している交通系 IC カードやプリペイド決済用 IC カード等，共通規格に基づいて発行されている一般カードを使い，身分・所属ごとに各システムを利用できるようにするための仕組みを提案する.

一般カードは，組織ごとに専用に作られたカードと異なり，認証用に新たに情報を追記することや，組織固有の暗号化された格納情報を認証に使用することが難しく，利用でき

る認証情報に制限があるためセキュリティ対策が必要になる．そのため，システムの重要性に応じて要求されるセキュリティレベルの格付けを行い，それに応じて設計を行う．

大学向け一般カードを使った認証は，著者らの先行研究として，認証情報にカード内の読取り可能情報を組合せて使用し，さらにはキー情報を追加して使用し，その情報を一元管理するための DB を構築するシステムの設計を行った[78]．しかし，NFC（Near Field Communication）機能搭載の携帯機器の出現により，IC カードをエミュレーションすることが簡単にできるようになり，読取り可能情報だけを認証に使用することは安全性が不十分となった．さらに，大学という組織の特徴より，一時利用者の情報を中央の DB で一元管理することは非常に困難であった．

これらより，本研究では，入退館システムなど要求されるセキュリティレベルが比較的低い認証システムは，一般カード内から読取り可能な情報を認証に使用する．これに対し，中程度以上のセキュリティレベルが要求されるシステムに対しては，カードの紛失や偽装の対策を考慮した認証システムとする．カード内の読取可能な情報だけでは不十分であるため，これらに加えて，本人のみ知り得るキー情報（以下，PIN（Personal Identification Number）コードとよぶ）による認証を併用する．

PIN コード認証を行う際，一般カード内には容易に情報を追加できないため，PIN コード情報を認証システム側に格納しておく必要がある．しかし，運用上の観点から，特に一時利用者向けとした場合は，認証に関する認証システムの負荷が一般利用者と同等以下であることや，管理に伴う人的コストが十分小さいことが求められること，利用者の管理部局は身分属性によって異なることより，カードの登録は分散して行いたいという要請がある．また，大学のような組織の特徴として，学部・学科等の部局ごとの特徴を出すため，部局ごとにシステムを管理していることや，離れた研究所等においてはネットワークが分離されている場合も多くあるため，各システムを中央で一元管理することは難しい．そのため，部局ごとに管理者が容易に管理できるシステムとすることより，格納する情報は必要最低限にするよう求められる．これらの問題を検討した結果，カードにも各認証システムにもカード固有の情報（カード ID）や PIN コード情報の登録を行うことなく，カードごとに異なる値を利用して PIN コードを生成する式だけを格納する，**PIN コード生成方式**を提案した．PIN コード生成方式は，カード内の読取可能情報から取り出したカードごとに異なる値にハッシュ関数を適用することにより，PIN コードを生成する手法である．この方式は，システム側にユーザ情報や PIN コード情報の登録を行うことなく，一般カードに対して，PIN コードを発行するだけで，一時利用者が利用可能になる．また，この方式は，中央で一元管理しないことにより，地理的にもネットワーク的にも離れた地域で

も，PIN コードさえ発行できれば，システムが利用可能となる．これによって，部局の管理者は PIN コードを管理することなく，一時利用者が保持する一般カードに対して，PIN コードを発行すれば，一時利用者はシステムが利用可能になる．

本研究は，大学間連携のための認証基盤が整備されつつある中，一般カードを用いた認証システムの大学間連携の実現を目指しつつ，IC カード認証システムの全学導入に向けて検討を行っていた東京海洋大学の品川キャンパス向けに，試験運用を行った．

3.2 関連技術

3.2.1 一時利用者と IC カード

大学のような分散管理組織では IC カードを導入する場合，一時利用者の扱いが課題となる．管理部局が分散されており在籍情報を集約することが難しい一時利用者に対して，着任する度に IC カードを発行し，離任の度に回収することは，運用管理の煩雑さやコスト面から非常に難しく現実的ではない．そのため，一時利用者に，施設利用時等の必要に応じて，白カードといわれるカードを貸出している組織もあるが，通常は，一時利用者に対してはカード発行等の対応をとらず，一時利用者が IC カードを使ったシステムが利用できない状態となっている組織が多く見られる．

IC カードを発行する際，カード発行のコストだけでなく発行後の運用管理の煩雑さも発生する．本研究では一時利用者に対しては運用管理の煩雑さやカード発行のコストを最低限におさえるため，一時利用者には IC カードを発行せず，本人が日常利用している交通系やプリペイド決済系の IC カードを使う．そして，一時利用者の身分・所属による利用可能な範囲で，組織ごとに専用に発行したカード（以下，専用カードとよぶ）の利用者と同様に認証システムが利用できるよう，各システムの重要性に応じてセキュリティレベルの格付けを行い，各認証システムが利用できるようにするための仕組みを提案する．本研究における一般カードとは，交通系 IC カードやプリペイド決済用のカード等，日常生活で簡単に手に入れて利用することができる共通規格に基づいたカードのこととする．

3.2.2 一般カードと専用カード

専用カードは組織ごとに安全性を考慮して作成するカードであるため，セキュリティは比較的高く，カード内情報の書き換えや独自に情報を追加することができ，また，券面表示もできるといった利点がある．このため，本来は専用カードだけで運用するのが望まし

い．しかし，大学などの一時利用者が多い組織においては，一時利用者の着任する度に専用カードを発行し，離職の度に回収することは，運用管理の煩雑さやコスト面から非常に難しい．一方，一般カードは，カード発行元において重要な取り決めがあるため，新たな情報の追加や，中身の書き換えすることが難しく，自由に新しいサービスを提供することが難しい．また，カード内情報の取り扱いにも制限があるため，認証に暗号化された情報を使用することが難しく，読み取り可能な情報を使用することになるため，セキュリティは比較的低くなる．しかし，一般カードの場合，カードを持っていればよく，新たにカードを発行し回収する手間やコストは削減できる．一般カードは，交通機関等で IC カードが発達している都心では，複数のカードを保持している人が多く，カードが増えることを好まない人もいる．そのような中で，新たに保持するカードを増やすことなく，現在保持しているカードで認証システムが利用できるようになることは，一時利用者の利便性が向上にもつながる．

3.2.3 一般カードを用いた認証システムの事例

FeliCa タイプの一般カードを使った認証システムとしては，カード内から読取り可能情報である製造 ID（IDm）等を抜出し，認証に使用する製品が販売されている．本章ではこれらの製品例を紹介し，さらに我々が行ってきた先行研究と課題，および一般カードをつかった認証方式について紹介する．

（１）一般カードを使用した認証システムの製品事例

大学における導入事例としては，FeliCa タイプのカードや FeliCa 機能搭載の携帯電話を使って，授業の出席管理等を行っている大学がある[79][80]．日常生活においては，交通系の IC カード（おサイフ携帯も可）を登録すると，提携した店や施設でかざすだけで，ポイントをためることができるシステムや[81]，FeliCa 搭載の携帯電話，運転免許証（IC カードのタイプは ISO/IEC14443 TypeB），taspo（IC カードのタイプは ISO/IEC14443 TypeA）カードなど身の回りの各種 IC カードで車キーやドアをロック・アンロックできる製品が販売されている[82][83]．これらのシステムは，カード内の読取り可能領域から情報を抜出して認証に使用しているため，安全性が求められるシステムにとっては，カードの盗難や偽装時に対する対応が少し足りないと考える．セキュリティレベルが中程度以上のシステムにおいては，カードをかざすだけの認証ではなく，悪用可能性の対応として，さらなる認証情報を組み合わせることが求められる．

（２）一般カードを使用した認証システムの先行研究

著者らの先行研究として，大学の一時利用者向けに，本人が所持している交通系の IC カードなど FeliCa タイプのカード（一般カード）を使って，それらを大学の IC カード認証基盤と結びつけるための仕組みの提案を行った．提案では，セキュリティレベルに応じて認証システムの設計を行った．セキュリティレベルが比較的低いシステムにおいては，カード内の比較的読取りが容易にできる製造 ID（IDm）による認証を用いた．セキュリティレベルが中程度のシステムにおいては，カード内の読取り可能な情報から複数の情報を組合せたもの（カードシステム ID と呼ぶ）を認証情報とし，比較的高いセキュリティレベルが求められるシステムにおいては，さらにキー入力を追加した認証を行った．

先行研究の時点では，FeliCa の IDm は簡単に読取ることができるが[84]，FeliCa タイプのカードはカードの複製が困難であると言われていたため，IDm 等が読み取られた場合でも，悪用の可能性が低いと考えていた．

また，一時利用者を一元管理することを前提に中央に認証ゲートウェイサーバを構築し，一時利用者のカード内情報もキー情報も中央で管理する仕組みとしていた（図 3-1）．

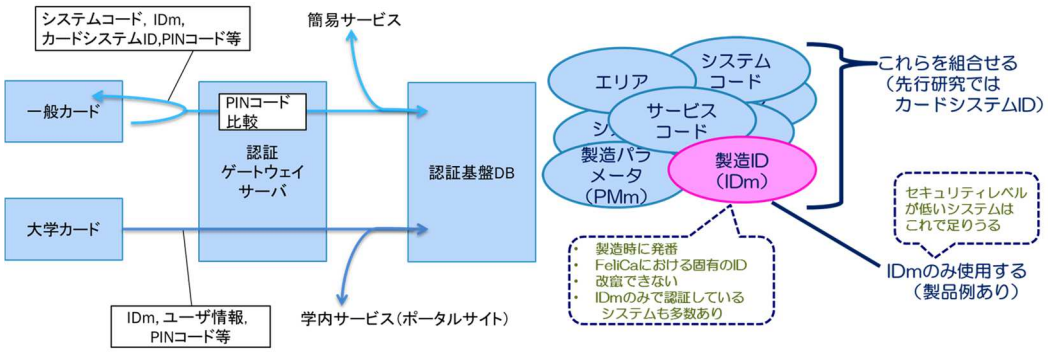

図 3 - 1　先行研究の認証図

先行研究を行っていた際，市場に出回っている携帯電話の多くは FeliCa 機能が搭載されていたが，近年は NFC 機能搭載のものが市場に出ている[85]．NFC 機能搭載の携帯電話は，リーダ機能も搭載されており，FeliCa カードをエミュレーションすることが簡単にできる．この技術は，IDm だけでなく，非暗号領域も簡単にエミュレーションできる．この技術が悪用された場合，NFC 機能搭載の携帯電話に FeliCa カードをかざすとカード内の読取り可能情報を取得し，携帯電話がそのカードに成りすますことができる．これらより，認証時に IDm だけではなくカードシステム ID を使用した場合でも，なりすま

しによる悪用の可能性が否定できないため，安全性の問題が出て来た.

そこで，カードシステム ID は，認証に IDm のみを読み取って偽装することは比較的簡単であるため，IDm のみを偽装する攻撃に対して，メリットがあることより，カードシステム ID は，IDm の補助的に使うこととし，セキュリティレベル中程度以上の認証方法を再検討することとなった.

また，2.2 のとおり，大学のような分散管理組織の特徴より，中央に認証ゲートウェイサーバを構築し，一時利用者情報や一般カード情報を管理することは難しく，一時利用者の利用システムの可否を中央で管理することは困難であった. 中央に認証ゲートウェイサーバを設置する場合，常に，認証システムとの通信が必要であるため，ネットワークが異なる場合や通信が遮断された場合, そのサービスが使用できなくなるという課題もあった. 大学で提供するサービスは，個別に独立して運用されていることも多く，特に，地理的に離れた山奥や離島，実習船内等では，中央管理のシステムと常時通信ができない場合も多いという課題もあった. 企業においても組織規模が大きくなると，独立した部局や離れた場所に研究所があり，情報システムも研究所ごとに管理している組織もある.

そこで，本研究で提案する IC カードを用いた一時利用者向け認証システムは，中央管理のシステムとして稼働せず，部局ごとに提供するサービスとして提案する. これにより，提案の仕組みは例えば船内 LAN 環境等においても利用可能となる. これらより，本研究においては，セキュリティレベルの重要度に応じた認証方法を再度検討し，さらに，中央で一元管理することなく，部局ごとに容易に利用できるシステムの提案を行った.

3.2.4 一般カードを使った認証方法

一般カードは組織ごとに専用に作られたカードではないため, 認証用に新しく情報を追記することが困難である. 一般カード内の格納情報から認証に使用できる情報と安全性の検討を行う.

A） FeliCa 内の情報を使った認証方法

FeliCa 内のメモリは以下の二種類のブロックに分かれており，それぞれ表 3-1 のような特性がある[86][87].

- **ユーザブロック**：ユーザデータが書き込まれる領域
- **システムブロック**：FeliCa の構成情報が保存されている領域

本来はユーザブロック内情報を使用する方がよいが，重要な取り決めが必要である．システムブロック内情報はユーザブロック内情報に比べて安全性は高くないが，取扱いは比較的容易である（表 3-1）．

表 3‐1　ユーザブロックとシステムブロック

ユーザブロック	システムブロック
・安全性高い ・（基本的には暗号化あり） ・相互認証あり ・カード種類によって格納されている領域が異なる ・暗号化領域の利用は，発行元と重要な取決必要	・安全性低い（基本的には暗号化なし，情報の読取可能） ・相互認証なし ・FeliCa であれば，格納されているブロックの領域は同じ ・中身の書き換えは基本的には不可

B） 一般カードを使った場合の安全性の考慮

一般カードを使った認証方法は，大きくは 3 つの方法に分けることができる（表 3-2）．

表 3‐2　一般カードを使った場合の認証方法

	認証方法	備考
1）	カード内に情報を追記	鍵情報等を格納
2）	カード内の情報を利用	① 暗号化領域を使用 ② 非暗号化領域を使用
3）	その他（[1]と[2]以外）の情報の組合せ	① 指紋や静脈認証 ② キー入力による認証

ここで，1）と 2）①の場合は，安全性が確保されるが，カード発行会社と重要な取り決めが必要なため，本研究においては検討を省略する．2） ②は，2.3.2 のとおり，先行研究において検討していたが，NFC 機能搭載の携帯電話による偽装問題がある．ただし，セキュリティレベルが比較的低いシステムにおいて使用すればよいと考える．

セキュリティレベルが中程度以上のシステムにおいては，3）を検討する．ここでは 3）①や 3）②があげられるが，個人情報の取り扱い等を考えると，比較的導入に抵抗がない 3）②のキー入力による認証が妥当であると考える．本研究では，この本人しか知りえないキー情報（PIN コード）の新しい生成方法，認証方法，それに伴う管理・運用方法を様々な方面から検討し，設計，構築を行う．

3.2.5 本研究で想定する IC カードを用いた認証システム

IC カードは，入退館システムや証明書発行システム，PC ログインシステム，各種情報システムの利用等で利用される． 本研究では，一時利用者が利用するシステムを表 3-3 と仮定し，これらのシステムの重要性に応じてセキュリティレベルの格付けを行い，それぞれのレベルに応じた認証システムの設計を行う．

表 3 - 3　本研究で想定するサービス

	想定するサービス	セキュリティレベル
(1)	建物の入退館時の認証	低
(2)	学内限定簡易 Web サイト学外から閲覧時の認証	中
(3)	学内限定ポータルサイト学外から閲覧時の認証	中上

（1）は，平日の日中であれば誰でも出入りできるが，平日の夜間や土日祝日にはカードをかざして出入りするシステムとする．重要部屋への出入りシステムではないため，カードの偽装の対応は考えないことと，備付けの専用カードリーダを使用するためシステム改ざんの可能性は非常に低いと考えることより，セキュリティレベルは比較的低く設定する．

（2）は，学内ネットワークに接続すれば誰でも閲覧可能な学内限定サイトを，学外ネットワークから閲覧する際に，カード認証を行うシステムとする．ここでいうカード認証とは，IP アドレスや共通パスワードによる制限のようなものと考え，Web サイトの内容は，重要情報ではなく，簡易な学内スケジュール等を掲載するサイトする．ただし，認証は個人 PC から行うため，システム改ざんやカード偽装等の対応を考慮することより，セキュリティレベル中程度とする．

（3）は，部局ごとに運用しているポータルサイト等とし，個人認証が必要であり，個々に表示が異なるようなシステムとする．（2）の認証だけではセキュリティレベルが不足する場合とし，カード認証の後に，さらなる認証として個々のアカウントとパスワードによる認証を追加する．

なお，本研究における一般カードとは，日本で交通系のカードとして一番利用されている Suica や PASMO 等の交通系 IC カードや nanako や WAON 等プリペイド決済用の IC カード等，日常生活で簡単に手に入れて利用することができる共通規格に基づいた

FeliCa タイプのカードに限定して設計および実装を行うが，本提案の基本的な考え方は他のタイプのカードでも広く応用できるものである．また，本研究で構築したシステムの利用者は，一時利用者に限らず，IC カード未導入の組織等の一般利用者でも利用可能である．

3.3 PIN コードを使った IC カード認証システムの提案

本研究では，入退館システムなど要求されるセキュリティレベルが比較的低い認証システムは，先行研究と同じく一般カード内から読取り可能な情報を認証に使用する．これに対し，セキュリティレベルが中程度以上を要求されるシステムでは，カードの紛失や偽装の対策を考慮した認証システムとするため，一般カード内の読取可能な情報だけを認証に使用するのは不十分であることより，本人のみ知り得る PIN コードによる認証を併用する．本研究では，セキュリティレベルが比較的低いシステムにおいては，製品例とほぼ同等であることより，セキュリティレベルが中程度以上のシステムを重点的に設計し，実装を行う．

なお，本研究で提案するシステムは，部局ごとに管理するサービスとすることより，各部局のシステム管理者の負担は最低限にする必要が求められる．

3.3.1 従来の PIN コードを使った認証方式

これまでの PIN コードを使った認証システムは，PIN コード情報を一般カード内に格納する方式，もしくは，認証システム内に格納する方式であった．これらの方式は，カードや PIN コードの登録・管理のためのコストが発生する．また，PIN コードを一般カード内に格納する方式は，安全性が確保されるが，それぞれのカード発行会社と重要な取決めが必要となることや，カード紛失時の悪用対策に格納情報の暗号化などが必要であるため，容易ではない．一方，PIN コードを認証サーバ内に格納する方式の場合，中央管理の認証サーバにカード ID や PIN コード情報を格納しておき，各部局が管理する認証システムから認証時に参照されることが求められる．しかし，その場合は，ネットワークが常に中央管理のシステムと接続されている必要があるが，大学によっては，中央管理のシステムとネットワークが独立している部局がある．また，中央管理のシステムにカード情報や PIN コード情報を登録する際，大学として把握できていない一時利用者の情報を登録することが困難であるという問題がある．

運用上の観点より，一時利用者が一般カードを使ってサービスを利用する場合，認証に

関する認証システムへの負荷は, 専用カード利用者の負荷と同等もしくはそれ以下であることが求められる．さらに，2.2.2 節のとおり，大学のような組織では，部局ごとにサービスを立ち上げて管理されていることが多いため, 部局ごとの管理者が容易に管理できるシステムが求められる．

3.3.2 新しい PIN コード生成方式の提案

上記より, 本研究においては, 各認証システムに格納する情報は必要最低限となるよう，PIN コード情報は，IC カード内や認証システム内に格納せず，IC カード内の固有の情報から一方向関数により PIN コードを生成する「PIN コード生成方式」を新しく提案する．

提案する PIN コード生成方式は，認証システム側にカード情報や PIN コード情報の登録を行わず, PIN コード生成式を格納するだけよいため, 従来方式に比べて利用者ごとの PIN コードの管理や登録作業が不要であり，比較的コストを抑えることができる（表 3-4）．ただし，PIN コードの値は自由に設定することができないため，運用でカバーする必要がある．

表 3 - 4　一般カードの認証方式と特徴

	PIN コード生成方式（提案方式）	認証システム内に格納する方式（従来方式）	一般カード内に格納する方式（従来方式）
管理コスト	小	大	大
登録作業	不要	必要	必要
安全性	中程度	高	高
PIN コード値	設定不可	自由に設定可	自由に設定可
その他	PIN コード発行だけでシステム利用可に	認証システム内に PIN コードの管理が必要	・カード発行会社と重要な取決が必要 ・カード紛失時の悪用対策に格納情報暗号化（コスト大）が必要

ここで，部局に設置した管理者用 PC 機器から Web 経由で中央の集中サーバにアクセスして PIN コードを渡すことも可能と考えられるが，2.2.3 節のとおり，本研究では，一般カードの受付と PIN コードの生成は, サービスを提供する部局ごとに行う設計である．この方式では，部局ごとに，独自の PIN コード体系を作ることができ，部局ごとの限定サービスとして提供することも可能となる．

3.3.3 PIN コード生成方式

PIN コードを生成する際に，PIN コードの値はカードごとに異なる必要がある．一般カードの読取り可能領域には，カードごとに異なる値が格納されているため，それらを抜出し，少し工夫を加えることにより，PIN コードを生成する．具体的な PIN コードの生成方法を以下に記す（図 3-2）．

生成式 ： SUBSTR（HASH（n ＋SALT），*position*，*length*）

（n：抜出した情報　*position*: 切出す文字の開始位置　*lengh*：切出す文字長）

図 3 - 2　PIN コード生成式

PIN コードの生成方法：

1．一般カードの読取可能な情報から値を抜き出す
　　（カードごとに異なる情報を含んだ値とする）
2．抜き出した情報を組み合わせる
3．SALT を付加する
4．HASH 化する
5．任意の桁数を抜き出す

この生成式では，一方向関数に秘密情報を組み合わせていることにより，カード内から抜出した情報だけからでは PIN コードの生成ができない．また，PIN コードが漏えいした場合でも，他の利用者の PIN コードは推測できないため，当該利用者以外への影響を防ぐことができる．

SALT を付加する理由は，SALT を付加せずにハッシュ化するだけであれば，ハッシュ関数は公開されているため，生成した PIN コードが漏えいしてしまう可能性がある．そこで PIN コード生成の強化のため SALT を付加する．また，SALT は PIN コードに有効期限をつける際に，SALT を変更することで対応する．

これにより，認証システム上で実装する際には，認証システム上には，PIN コードを生成するための式と，生成した PIN コードと入力した PIN コードを照合するための式だけを格納すればよくなる．認証システム上での実装方法については，2.5 節で記す．

3.3.4 PIN コード運用手法

PIN コードを運用する際に，悪用される可能性を最小限にするため，運用における工夫が必要となる．以下，PIN コードを使った認証システムに対して，起こりうるインシデントのパターンとリスクを分析し，それに対する対応，コストを比較し，実現可能性を検討する．起こりうるインシデントとしては以下の 3 パターンを考える．

- パターン 1：カードの紛失・偽装
- パターン 2：PIN コードの紛失・漏えい
- パターン 3：カードの紛失・偽装と PIN コードの同時紛失・漏えい

I. カードの紛失･偽装に対する対策

基本的にはカードだけでは，PIN コードが分からなければ利用できないため，新しいカードで PIN コードを発行すればよい．悪用の可能性がある場合はカード失効処理を行う．

ただし，カードの取得者・偽装者による PIN コードを何度も試してのブルートフォース攻撃が心配されるため，PIN コード認証には入力制限をつけておく．入力制限にかかると，該当カードよりカード失効処理に必要な情報を抜出し，管理者に警告を上げるシステムにしておくことで，管理者側でカードの失効処理をする必要があるかの判断を行う．これらは，通常の運用コスト以外に，悪用可能性時のカード失効処理と，警告がある際に，管理者が作業するコストが発生する．

II. PIN コードの紛失･漏えいに対する対策

基本的には PIN コードだけでは，カードがなければ利用できないため，単に PIN コードを忘れただけの場合は，再発行を行う．悪用の可能性がある場合は，該当カードに対してカード失効処理を行う．

ただし，離任した人がいつまでも使えたり，知らない間に悪用されていたり等のリスクを最低限に抑えるために，PIN コードの生成の種を定期的に更新し，PIN コードを配布し直す．定期的な期間が短いと多くのコストが発生するため，更新は年に 1 回か 2 回程度とする方がよいと考える. PIN コードの更新時には失効処理情報も一新し，失効処理していたカードも申請し直すことで，新しい PIN コードで利用できる．通常の運用コスト以外に，悪用可能性時のカード失効処理と，定期的に PIN を生成し，配

布するためのコストが発生する．

III. **カードの紛失・偽装と PIN コードの紛失・漏えいに対する対策**

これはⅠ，Ⅱに比べて，緊急性が高いため，直ちに失効処理を行う．この場合，緊急対応のためのコストが必要となるが，カードと PIN コードの両方一度に紛失することは滅多に起こらないと考えるため，通常運用においては滅多にコストは発生しないと考える．

これらより，認証システムには，PIN コードの入力制限をつけることと，カード失効処理のために失効リストを作成しておき，失効の度に追加できるようにしておく必要がある．失効リストに登録する情報は PIN コード生成に必要なカード内情報の一部であり，カードごとに異なる情報を含んだ値とする．

また，PIN コードの更新と失効リストの更新時期は 1 年のうち人の入れ替わりが一番多い年度末にするのが良いと考える．

3.3.5 カードおよび PIN コードの失効，更新処理

失効処理は頻繁に発生するものではないが，認証システムの利用ユーザ情報はシステムごとに管理するため，失効リストは認証システムごとに格納する．各認証システムにはあらかじめ失効リストを作成しておき，失効処理の際に追加する．失効処理の際に登録する情報はカード内情報とし，カードに対して失効処理を行う．PIN コードはカードと一対であるため，カードが失効していれば，PIN コードも使用できないことより，PIN コードの失効処理はカードの失効処理と同様にカード内情報を登録する．

悪用の可能性を減少させるため，PIN コードには有効期限をつける．有効期限ごとに SALT を変更し更新する．PIN コードの有効期限の更新は，SALT を変更し更新する．PIN コードの更新時には 2 週間～1 ヶ月程度の更新手続き期間を設定し，その間に継続利用する一時利用者は新規申請時と同じ手続きを行い，新しい PIN コードを受領する．

更新作業の便宜上，更新手続き期間中のみ，今まで使用していた PIN コードと新しい PIN コードを利用可能とする．PIN コードの更新時に合わせて失効リストの更新も行うため，PIN コードの有効期限更新後，新たに PIN コードを発行することにより，失効処理されていたカードも利用可能とする．PIN コードの失効処理が行われたカードに対しては，PIN コードを再設定方法も考えられるが，最近は一般カードを多数保持している人

が多いため，失効処理が行われたカードに対しては，一旦使用不可とし，新カードを登録し直してもらい，PIN コードの有効期限更新後，新たな PIN コードで再度利用可能とする．

3.4 PIN コード生成方式を用いた認証システムの実装

上記の設計を元に実装を行う．本システムは，2.2.2 節の大学のような組織の特徴より，部局ごとに管理されるシステムで比較的容易に運用できるよう，部局ごとのシステム管理者は，重要な情報の管理が不要なシステムであり，PIN コードさえ発行すれば，利用可能となるシステムとする．中央管理のシステムで一元管理を行わず，認証システムごとに，PIN コード生成プログラムと PIN コード認証プログラム，SALT と失効リストを格納することで，組織のネットワークと異なる場所にある部局でも，独立して運用が可能となる．

3.4.1 本研究におけるセキュリティレベルの設定

セキュリティレベルの制定は組織によって異なるが，本研究では，セキュリティレベルを表 3-5 と制定し，これを元に実装を行う．利用するシステムとそれに対するセキュリティレベルを 4 段階に分け，セキュリティレベルは認証における安全性の重要度に比例して高くなるよう設定する（表 3-5）．

表 3 - 5　一般カード利用によるセキュリティレベル表

セキュリティレベル	認証に必要な情報	利用サービス例	備考
4 (高高)	----------	人事システム 予算システム等	重要システム， 一時利用者利用不可
3 (中上)	読取可能情報(IDm 等) PIN コード， ID，PWD（個人認証用）	情報システム (個人認証付ポータルサイト閲覧)	個人 PC 利用
2 (中)	読取可能情報(IDm 等) PIN コード	情報システム (簡易 Web 閲覧)	個人 PC 利用
1 (低)	読取可能情報(IDm 等)	入退館システム	固定専用リーダ

セキュリティレベル 4 は，専門の常勤職員のみが利用するような重要システムとするため，一時利用者の利用範囲は 1～3 とする．セキュリティレベルが比較的低いシステム（セキュリティレベル 1）については，カード偽装の恐れ等は考慮しないことより IDm 等のカード内の読取可能情報を使った認証方法とする．セキュリティレベルが中程度（セ

キュリティレベル 2）以上のシステムは，カード偽装等の恐れを考慮することより，カードと本人のみ知る PIN コードを併用する．ただし，PIN コードを使った認証は，2.2.4 のとおり，IP アドレスや共通パスワードによる制限のようなものと考える．セキュリティレベルが中上のシステム（セキュリティレベル 3）では，セキュリティレベル 2 の IC カードと PIN コードによる認証だけでは不足すると考え，さらに個人認証が必要とするシステムとすることより，IC カードと PIN コードによる認証後，Web 上での ID とパスワード認証を行うものとする．

なお，セキュリティレベル 1 の認証方法については，既に商品化されているものがあることより，本章では省略し，ここでは，新しく提案する PIN コード生成方式を使用するセキュリティレベルが中程度以上のシステムについて重点的に記す．

3.4.2 セキュリティレベル２と３の認証方法

セキュリティレベル 2 と 3 の認証方法の流れは以下になる（図 3-3）．

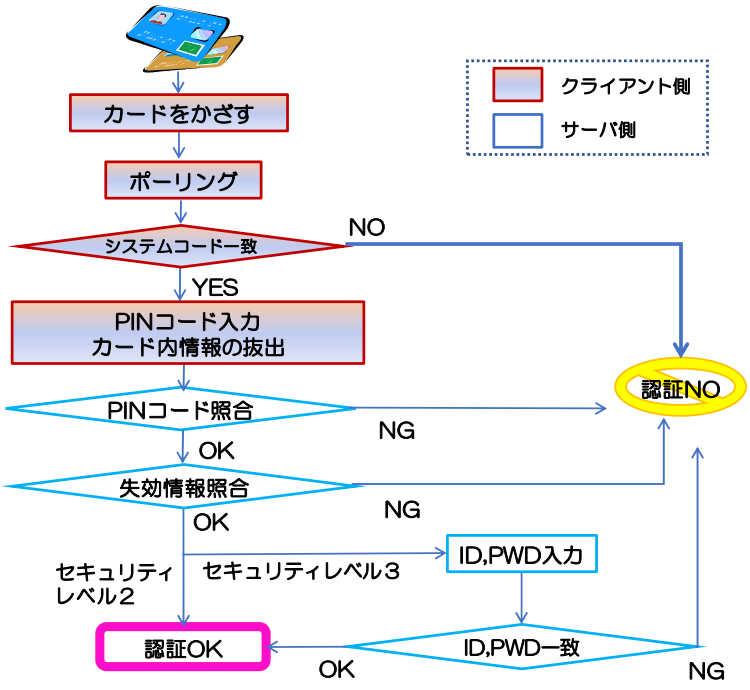

図 3 - 3　認証の流れ

1）　認証用 Web ページを開く

2）　カードをリーダにかざす

３） システムコードをチェックする

４） PIN コードを入力する

５） PIN コード生成に必要なカード内情報を取得し，PIN コードの照合する

６） 失効情報の照合する

７） 失効情報に情報がなければ認証に成功で，サービス利用可能となる

※さらに，セキュリティレベル３では，以下の認証方法を追加する

８） ID とパスワード入力し認証を行う

９） ID とパスワードが合致すれば，サービス利用可能となる

3.4.3 PIN コード生成方式による PIN コード発行フローと認証フロー

認証システムの中には PIN コード生成用のプログラムと PIN コード認証用のプログラム，および SALT と失効リストを格納し，それぞれ，www 上からアクセスする．開発環境には，SDK for NFC Adobe AIR Flash Basic 1.3.0，Perl 5.16 を用いる．PIN コード発行フロー，PIN コード認証フローを以下に記す．

A） PIN コード発行システム

管理者用 PC から www 経由で認証システムの PIN コード発行用 URL（管理用）にアクセスし，PIN コード発行画面を表示する．PIN コード発行画面が表示されるとカードリーダに一般カードをかざし，カード判別を行う．カード判別に成功すれば，カード内から PIN コード生成に必要な情報を抜出し，認証システムに送る．認証システム側では送られてきた情報に SALT を付加して，PIN コードを生成し，PIN コード情報を返す（図 3-4）．

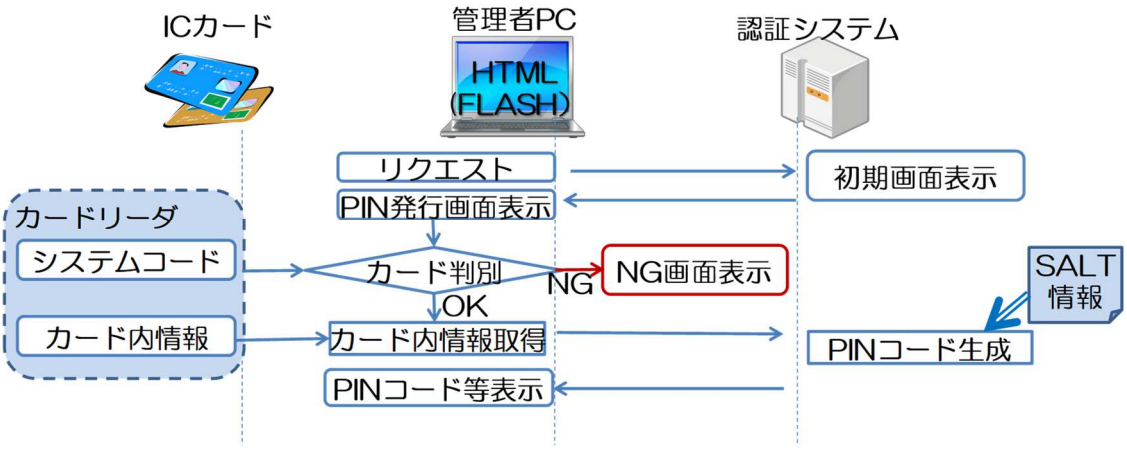

図 3 - 4　PIN コード発行システムのフロー

B)　PIN コード認証システム

個人 PC から www 経由で認証システム URL にアクセスし，ログイン画面を表示する．ログイン画面で表示されるメッセージ（「カードリーダに一般カードをかざしてください」）に従い，カードをかざす．カード判別を行い，カード判別に成功すれば，PIN コード入力を行う．入力された PIN コードとカード内から PIN コード認証に必要な情報を抜出し，認証システムに送る．認証システムでは送られてきた情報に SALT を付加して PIN コードを生成し，入力された PIN コードと比較する．PIN コードが合致すれば，失効処理情報の確認を行う．抜き出した情報の一部と失効リスト情報を照合し，失効リスト情報と合致しない場合は，認証成功となる．

PIN コード照合が成功しない場合，入力制限回数までは，PIN コードの入力ができるが，入力制限数を超えた際に NG 画面を表示し，カード内から失効処理に必要な情報を抜出し，管理者にアラートを上げる．また，図 3-5 の右の点線箇所は有効期限の更新期間に，繰り返し処理をする範囲であり，PIN コード更新期間は SALT を 2 つ持たせ，2 つの PIN コードで認証できることとする．

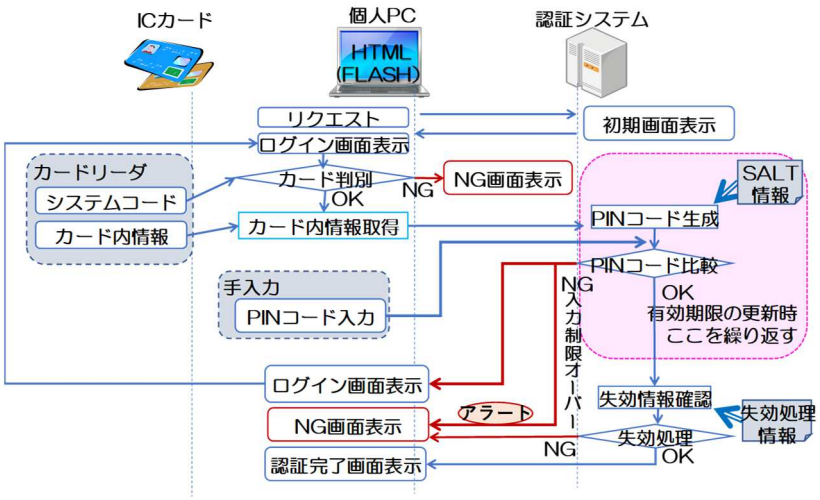

図 3 - 5　PIN コード認証システムのフロー

3.5 IC カードを用いた認証システムの試験運用と評価

3.5.1 試験運用に向けて

本研究で提案する仕組みは，IC カードが全学導入されており，その中で IC カード発行が困難な一時利用者向けに提案するシステムであることが前提であったが，要求するセキュリティレベルに応じて一時利用者向けだけではなく，IC カードが導入されていない組織にも応用することができる．

そこで，本研究で実装したシステムを，学生に対して IC カード学生証を発行しているが，教職員に対しては，IC カードは発行しておらず，導入検討中の段階であった東京海洋大学にて試験運用を行った．

3.5.2 セキュリティレベル 1 の試験運用と評価

東京海洋大学品川キャンパスの 1 建屋の入退館システムにおいて，セキュリティレベル 1 を実装し，試験運用を約 1 年間行った．システムの登録件数約 200 件であり，そのうち一般カード利用者は約 50 件である．認証は IDm のみを使った認証とし，既に製品も販売されていることより，認証方法の説明は省略する．入退館システムでは，建物ごとに入館できる人を区別する必要があるため，システムには個別に申請に応じて IDm とユーザ情報を格納した．

試験運用を行った約 1 年間，運用でカバーできる問題が 3 件発生したのみで，大きな

問題は発生しなかった．一般カードの登録時に，1 件，清掃業者は個人ではなく清掃業者として契約しているため個人カードは利用したくないとの希望があり, 白カードを発行して対応した．さらに運用していく上で，2 件，Suica 等のカードが，自動で新しいカードに変更されていることがあり, ユーザが気付かずカードが使えないことがあった. これは, 交通系のカードではカードが変更になることを意識してもらうよう周知する等, 運用でカバーする必要がある．今回の試験運用で一般カードを使用した約 50 名の中には，一般カードを保持していない人はおらず, また一般カードを使用することに抵抗を感じる人はいなかった．また，運用においても大きな問題は発生しなかった．

3.5.3 セキュリティレベル２と３の試験運用と評価

東京海洋大学品川キャンパスの 1 部局にて，セキュリティレベル 2 と 3 のサービスの試験稼働を行った．IC カードが発行されていない約 15 名程度の教職員向けに，セキュリティレベル 2 としては，該当部局内で利用している学内限定のお知らせが記された Web ページを学外からアクセスする際に一般カードと PIN コードによる認証を行った．

セキュリティレベル 3 としては，該当部局で使用している学内限定のポータルサイトに学外からのアクセスする時に一般カードと PIN コードによる認証を行い，Web ブラウザ上での ID とパスワード認証を併用した．

本試験稼働における環境は，該当部局にて既に稼働している Web サイトに対して，既存システムに手を加えないよう，認証システムを別途構築し，個人用 PC から一般カードと PIN コードを使って認証する．具体的には，リバースプロキシサーバ[88]を構築し，その上で，3.4 節で実装した PIN コード認証用のプログラムを置く（図 3-6）．利用者は，リバースプロキシサーバ上の指定する URL にアクセスすることで，PIN コード認証画面が表示され，PIN コード認証に成功すると学内限定の Web サイトや学内限定のポータルシステムのログインページが表示される．

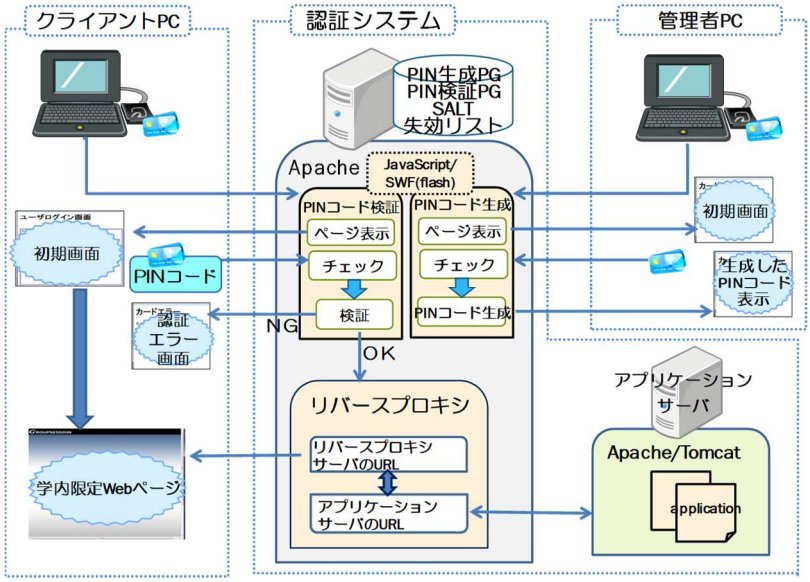

図 3 - 6　セキュリティレベル 2 と 3 の構成図

なお，試験稼働を行った際のそれぞれの環境は，個人 PC の OS は Windows7 と XP，利用ブラウザは IE，Firefox，GoogleChrome，利用リーダは Pasori リーダ，型番は RC-330，360，370 であった．これらの環境においては，大きな問題は発生せず，正常に稼働していた．ただし，Pasori リーダは，初めて PC に接続する際に自動的にドライバーをダウンロードする仕組みがあり，ネットワーク環境が不安定な場合，ドライバーがダウンロードされず，正常に動作しないことがあるため，運用でカバーする必要があると考える．

3.5.4 試験運用の全体評価

セキュリティレベル 1 の試験運用では，利用者からの申請に応じて IDm とユーザ情報を登録する作業が必要であるが，セキュリティレベル 2 と 3 の試験運用では，利用者には PIN コードの発行処理を行い，PIN コードを通知するだけでよい．システム管理者は PIN コード生成方式を使うことにより，利用者情報の管理が不要となることより，管理運用コストは抑えることができる．

本研究で提案する仕組みは一時利用者向けであるが IC カード未導入の組織や，IC カードが導入されている組織においても，応用できる仕組みである．現在，東京海洋大学では，学生向けに IC カードが導入されているが，教職員向けに IC カードは導入されていない．学内限定 Web サイトの学外からのアクセスの希望があるが，ID とパスワードによる認証だけでは安全性が確保できない可能性があることより，さらなる認証の強化が求め

られていた.

このような組織においては，教職員が普段利用する一般カードを使用し，セキュリティレベルにより本研究で提案するシステムを利用することで，さらなる認証の強化が実現されることが期待される.

3.6 実装したシステム全体の評価

本研究で実装した認証システムでは，ユーザ情報やカード情報は保持せず，PIN コード等の管理は不要である．そのため，従来の IC カードを用いた認証の仕組みに比べると管理運用コストを抑えることができる．本研究で提案する仕組みを用いることで，着任の度に行う必要があったカード情報の登録，PIN コードの発行，登録情報の管理，離任時の失効などの一連の操作が省略可能となる．具体的には，省略可能になる操作には，それぞれ申請書の管理や作業に対するダブルチェックなどを必要とすることより，一時利用者 1 人に対して一連の流れを行うことにより，約 1 人日の作業コストが必要になると想定するが，これらが削減可能になる．また，カードを発行しないことにより，カード本体のコスト以外に，カードの発行から管理，失効までにかかる運用コストが削減可能となる．これらの操作もそれぞれ申請書の管理などの操作が必要となることより，一時利用者 1 人に対して約 1 人日と想定する．一時利用者に対して，カード発行を行わず一般カードを用いて本研究で提案する仕組みを用いることより，カード本体のコスト以外に，運用コストが一時利用者 1 人につき約 2 人日削減できることになる．さらに具体的に，カード 1 枚当たりの本体価格を 2,000 円とし，作業に関する 1 人日を 10,000 円と仮定すると，1 人につき約 22,000 円が削減可能になる．1 年間で IC カードを用いた認証システムが必要な一時利用者が 100 人存在すると仮定すると，1 年間で 2,200,000 円削減可能になる.

本研究では，セキュリティレベル 2 は，学外から個人 PC より Web サイト閲覧するための認証システムを想定した．認証システムには，ユーザ情報や PIN コード情報は格納せず，PIN コード生成式のみ格納する．ただし，失効処理を行ったカードについてはカード内の一部の情報を格納する．これらは，2.2.4 節で記した通り，組織内ネットワークを IP アドレスや共通パスワード等によりアクセス制限しているものを，組織外ネットワークからは一般カードと PIN コードの所持者であれば全員アクセスを許すような運用である．つまり，一般カードと PIN コードの所持者のうちこの人とこの人だけに見せたい，というような利用制限はしていない．そのため，カード内情報や PIN コード情報を，利用者が追加されるごとに登録して管理する必要はないと考える．一度発行した PIN コー

ドは，失効処理を行わない限り，有効期限内は利用可能であるが，離職した人でも組織内ネットワークに入れば，利用できるシステムであるため，離職後に PIN コード有効期限は利用できても問題ないと考える．

セキュリティレベル 3 におけるメインの認証は ID とパスワード入力であり，その前段として PIN コード入力による認証を行っているため，セキュリティレベル 2 と同様に，認証システムにはカード内情報や PIN コード情報を格納することなく，利用者が追加される度に登録処理を行わなくてもよいと考える．ただし，本システムにおける PIN コードは，カード内情報を元に発行した値であり，ユーザが指定したものではないため，ユーザが忘れる可能性がある．そのため，運用方法の検討が必要となる．

また，実装したシステムでは，失効処理されたカードは，更新期間まで利用できないため，新たなカードに PIN コードを発行して利用する．交通機関等で IC カードが発達している都心では，複数のカードを保持している人が多く，この運用方法でよいと考えるが，カードが発達していない地域では，失効処理後の扱いにおいて再検討が必要となる可能性もある．ただし，カードや PIN コードの悪用，カードと PIN コードの同時紛失は，非常に少ないと考え，本研究では検討は省略した．

3.7 結語

本研究では，一時利用者に対する管理運用の煩雑さおよびカード発行に関するコストを最低限に抑えるため，一時利用者には IC カードを発行せず，一般カードを使って，身分・所属ごとにそれぞれのシステムを利用できるようにするための仕組みを提案した．

それぞれのシステムに対しては，安全性確保のために，システムの重要性に応じてセキュリティレベルの格付けを行い，セキュリティレベル中程度のシステムを重点的に，設計，実装を行った．セキュリティレベル中程度のシステムで実装した PIN コードを使った認証方法は，PIN コード発行システムで PIN コードを発行するだけで，システムが利用可能となり，システム管理者はユーザや PIN コード情報の管理が不要であり，容易に運用できる新しい PIN コード認証方法を提案した．セキュリティレベル 1～3 において試験稼働を行った結果，大きな問題は発生せず，本研究の一般カードを使った認証システムにおいて，表 3-5 で分類した 4 段階のセキュリティレベルのうち，一時利用者に求められるセキュリティレベル 3 までの安全性が確保できることが確認できた．

大学の組織の特徴より，一時利用者の全体数の把握は難しい．東京海洋大学において一時利用者の人数の確認を行ったところ，正確な全体数を把握できないが，1 年間において

把握できる一時利用者数は，全利用者の約 2 割であろうと言われている．また，IC カード身分証の 1 枚あたりの単価は 3,000 円前後であり，IC カードを発行すると発行手続きや失効に関する手続き，日々の管理において，運用コストが発生する．一時利用者は 1 年間に数百名から大学の規模により数千名の在籍が予想されることより，本システムの導入コストは発生するが，中長期的に運用することにより，コストが下がり運用の効率化につながる．また，一時利用者も IC カードを使ったシステムが利用可能になるため，利便性が向上する．

本研究における提案システムは，通常のカードリーダ以外には特別なハードウェアを必要としないシステムであり，導入コストは比較的小さい．また今回の提案システムは一時利用者向けに設計を行ったが，専用カードを導入していない組織において全利用者を対象に使用するなどの応用も，対象とする認証システムのセキュリティレベルによっては可能であり，広範囲で利用され普及することによりさらなるコストダウンも期待できる．

本研究における実装は，FeliCa で行ったが，今後，他のタイプの IC カードでも利用できるようにすることにより，他社や他大学における IC カード身分証が利用可能となる．近年，大学間連携のための認証基盤サービスが整備されつつある中，今後，大学間連携のための認証基盤サービスにも他大学所属の学生が所属大学の学生証でも利用できるようなシステムとして展開していくことが望まれる．

第4章　統合 ID と属性を用いたグループ管理

4.1 緒言

教育や研究，業務や日常生活などにおいて様々な仕組みがオンライン化され，大学などの組織では情報システムは必要不可欠なものになっている．オンライン化されたサービスは，サービスごとに個別に発行されていた ID が，組織において統合化される統合認証基盤の整備が進んでいる．

統合認証基盤に関しては，認証情報の統合化や管理の効率化に向けた研究が多くなされている．また，それらの技術を用いた組織間認証連携に対する研究も進められている．しかし，認証と連動してアクセス制限などを行ういわゆる認可の統合化については，依然として十分な普及に至っておらず，認証情報が中央の認証用のサーバ（以下，認証サーバとよぶ）で一元管理されるようになっていても，認可のために必要な情報はサービスごとにばらばらに管理されるのが一般的である．認可情報としては，サービスごとにアクセスを許可するユーザリストとして保持するか，認証サーバに格納されている属性の値に基づくか，あるいはこれらを組み合わせて指定し，それらに対してアクセス権限を設定するのが一般的である．しかし，中央の認証サーバに格納されているユーザの属性は，組織において共通に定義されているものであり，認証サーバの属性を指定するだけでは，各サービスが求める詳細なアクセス制限を行うことが難しい．また，各サービスの認可で使用するユーザの集合（以下，認可ユーザとよぶ）はサービス間で共通ないし重複する場合も多く，サービスごとに管理するのでは非常に効率が悪い．そのため，認可情報についても中央で統合的に管理できる仕組みが求められている．

本論文では，統合認証基盤が整備されている大学のような組織において，グループ機能を用いて，統合的に認可ユーザを管理する仕組みについて論ずる．著者らは，本研究の初期段階としてグループを効率的に管理できるようグループの体系化を行った[89]．体系化したグループに対して，実運用と合わせて効率的に管理する仕組みを提案し，提案する仕組みを「グループ管理システム」として実装し，試験的に運用を行った．

グループ管理の仕組みについては古くから検討されているが[90][91]，最近のものとしては，統合認証基盤と連携した分散管理の環境のために設計された米国の Grouper などが代表的である．しかし，Grouper などの仕組みでは，グループの管理を柔軟かつ詳細にするほど，そのシステム全体の管理を行う人（以下，システム管理者とよぶ）や各グループの管理を行う人（以下，グループ管理者とよぶ）の負担が大きくなる．本論文で提案する仕組みは，統合認証基盤と連携したグループ管理の仕組みにおいて，既に開発されてい

る Grouper などのシステムを実運用と照らし合わせ，グループに対する柔軟性やグループの継続性などの課題がシステム管理者からグループ管理者への権限移譲にあることを明確にした上で，それを解決しつつ，システム管理者およびグループ管理者の管理の負担を軽減する仕組みとする．

グループ管理の権限をシステム管理者からグループ管理者に移譲する際，プライバシーや個人情報保護などの要請により，属性などの取り扱いは，厳密な管理が必要となる[92][93]．そのため，通常はグループ管理者ごとに，参照できるユーザやユーザ属性の範囲の設定が必要となる．たとえば Grouper においては，グループ管理者に設定されたユーザやユーザ属性などの情報を参照する権限（以下，参照権限とよぶ）の範囲内でのみグループのメンバ管理が行えるという制約を課している．そのため，グループを定義する際にはそのメンバの範囲とグループ管理者の選任に制約があり，特に組織横断型のグループのグループ管理者になれる人は非常に限定されてしまう．また，グループ管理者ごとの参照権限の設定は，グループ管理者が交代する度に操作が必要となり，システム管理者に対する負担が大きい．

それに対し本研究で提案する仕組みは，グループ管理の権限を一般ユーザにも拡張し，参照権限にとらわれない柔軟なグループが作成できるものとする．グループ作成の度に，システム管理者がグループ管理者およびグループ管理者に対する参照権限を設定するのではなく，あらかじめユーザ属性ごとにグループ管理者の参照権限を条件式として設定しておく．そして，参照権限の範囲を越えたユーザをメンバにする際には，直接入力や条件式から導いたメンバを閲覧不可にすることで安全性を確保する．これにより，グループに対する柔軟性が増し，一般ユーザにグループ管理者になる権限を移譲することでシステム管理者のグループ管理の負担も軽減される．

一方，これまでのグループ管理の仕組みでは，グループが組織において公式のものかどうかやその重要度に関わらず，グループ管理者が転出等で不在になった際にグループが自動的に削除され，継続が必要な場合はシステム管理者が個別対応を行う必要がある点で，システム管理者の管理の負担が高かった．

本研究では，グループの重要度に合わせ，業務などで継続性の確保が必要なグループを「公式グループ」，通常のグループを「一般グループ」と区別する．公式グループでは，グループ管理者が不在とならないように，システム管理者がグループ管理者の管理を行う．グループ管理者の交替時にはスムーズに変更できるよう，グループ管理者は個々に登録するだけでなく，属性から導くこともできる仕組みとする．

本論文で提案する仕組みをグループ管理システムとして実装し，システム管理者からグ

ループ管理者へ, グループ管理者から新グループ管理者へ効率的な権限移譲が行えるようにした．実装したグループ管理システムは，LDAP Proxy 機能を用いて実装し，東京海洋大学で複数の Web サービスと連携しつつ 3 年間試行的に運用を行った．一般グループでは，一般ユーザが自由にグループを作成し管理することを許し，公式グループではグループ管理者を属性で指定できるようにしたことより, システム管理者やグループ管理者の管理の負担が削減され，運用コストの削減にも繋がることが確認できた．

4.2 関連技術

大学などの分散管理組織で提供されるサービスにおいて, 学部や学科などの単位で提供されるサービスは，利用者の ID 管理に対する負担軽減のため，ID を統合化し中央の統合認証システムと連携することが増えている．しかし，中央で管理する統合認証システム上には, 部局等で管理されるサービスのアクセス制限に使用するための詳細な属性がない場合も多く，サービスごとにアクセス制限は様々であることより，中央では認証だけを行い，認可はサービスごとに行われる場合が多い．部局等で管理されるサービスの中には，アクセス制限が重複するユーザも多くいることより, これらをグループとして管理することで，各サービスのアクセス制限の管理の負担を軽減する．

4.2.1 グループの体系化

グループは，グループごとに用途や作成時期，消滅時期，メンバの管理方法などが異なることや，1 人が複数のグループに所属するなど管理が複雑である．そこで，本研究の初期段階として我々は，グループを「ユーザの集合とそれを管理する人（グループ管理者）の集合の組」とし，複雑なグループを効率よく管理できるようグループの体系化を行った[89].

2.4.2 のとおり，グループを作成，管理する方法としては，個々にメンバを列挙して作成する方法，属性から導いて作成する方法，前者と後者を組合せて作成する方法がある．本研究では，これらのグループをそれぞれ列挙型，属性型，複合型と呼び，メンバ登録方法を表 4-1 のように定義し，メンバ登録の例を表 4-2 とした．

また，グループは，グループに対する管理の権限をグループごとの管理者に移譲することが必要であること，また，権限が移譲されたグループ管理者の管理の負担を軽減できるよう，グループには，ユーザを列挙するだけでなく，ユーザ属性や既存のグループからも導けることが必要である．

表 4 - 1　グループ作成時に必要とされるメンバ登録方法

呼称	登録方法
列挙型	メンバのリストを列挙する
属性型	属性（数値や文字列等）に関する条件式（=，＜，＞等）と それらを組み合せる論理演算（and，or, not 等）から導く
複合型	すでに作成されているグループを集合演算 (和集合，積集合，差集合，補集合)により導く

表 4 - 2　メンバ登録の例

呼称	登録の例
列挙型	groupAA = userA , userB, userC
属性型	groupBB = ("N**"="n**") and ("N**"≧"0")
複合型	groupCC = groupAA and groupBB

(group**=グループ名　N**=属性名　n**=属性値)

4.2.2 既存のグループ管理の仕組みと課題

Grouper などのこれまでのグループ管理の仕組みでは，システム管理者からグループ管理の権限を移譲された人がグループ管理者となり，グループやメンバを登録する．

システム管理者がグループ管理の権限を移譲する際, グループ管理者ごとにユーザやユーザ属性に対する参照権限の設定を行う．グループ管理者に任命された人は，与えられた参照権限の範囲内において，グループの作成，メンバ管理などを行う．作成されたグループのメンバは，グループ管理者に与えられている参照権限の範囲内であるため，属性型や複合型により導かれたグループのメンバリストを参照することもできる. グループ管理者がメンバを登録する際, 参照権限の範囲内のユーザリストや属性からメンバを選択し登録する. 複合型の場合は, 参照可能なグループのリストから組み合せるグループを選択する．

グループ管理者やメンバとして登録されているユーザが, 退職などにより統合認証システムからユーザ情報が削除されれば，グループ管理者やメンバからも削除される．そのため，グループ管理者やメンバがいつの間にか不在になる場合がある．そして，グループ管理者の全員が不在になった場合，通常は，グループは自動的に削除される仕組みとされている．グループ管理者が不在となり管理されなくなったグループを直ちに削除せず，年に

1 回程度不要グループを削除するなどの運用をしている場合もある. なお, Grouper では, グループ管理者は複数名登録可能であり，追加や変更時は列挙型により操作する.

本研究では, 既存のグループ管理の仕組みと実運用と照らし合せた際に, 比較的大きな課題となる以下の 2 点の課題について取り上げる.

一つは，グループの柔軟性が低いことである. 既存のグループ管理の仕組みでは，グループ管理の権限をシステム管理者からグループ管理者に移譲する際に, グループ管理者ごとに設定された参照権限の範囲内でメンバ登録を行うため, 作成されたグループは非常に限定的なものになる. また，システム管理者は，グループ管理者の新規登録時や交替時, 参照権限が変更になる度に対応が必要であり，グループが増えるほど負担が増える.

分散管理組織では, 例えば学生情報の管理は学生担当掛, 教職員情報の管理は人事担当掛，派遣社員の管理は契約担当掛など，それぞれの身分や所属により担当掛（以下，ユーザ担当掛とよぶ）が異なる. 組織の全利用者を横断的に管理するための掛は存在しない場合が少なくない. Grouper などを実運用する際にも, ユーザ担当掛以外の一般のユーザに対してグループ管理の権限を移譲されることはほとんど無く, ユーザ担当掛にグループ管理の権限を移譲しても制限が多く組織横断型のグループや詳細なグループの作成ができないため, 実際は, システム管理者がグループ管理を一元して行う場合が多い[94][95][96]. これらにより, グループ管理者やグループが増えるほどシステム管理者の管理の負担が高くなっていた.

もう一つは, グループの公式性や重要性に関わらず継続性が確保されていないことである. グループ管理者が不在になり管理されなくなったグループを残すと，リソースの無駄であるだけでなく誤用や悪用によるセキュリティインシデントにつながる懸念もあるため，通常はグループ管理者が不在になったグループは速やかに削除される. しかし，実際に業務などで使用するグループに対してグループ管理者が不在になったことにより直ちに削除されると，業務に大きく支障をきたす場合も多々ある. そのような場合，システム管理者に新たにグループ管理者を設定するような個別対応が求められる. このような運用では，グループ数が増えるほど，システム管理者の負担が増える.

4.3 効率的な権限移譲が可能なグループ管理システムの提案

本研究では, 統合認証基盤と連携したグループ機能を用いて, 統合的に認可ユーザを管理する仕組みを提案する. グループを管理する仕組みにおいては, 古くから検討されているが，本研究では，2.2 節で提起した既存のグループ管理の仕組みの課題を解決すること

で，システム管理者からグループ管理者，グループ管理者から次のグループ管理者へスムーズに権限移譲を行うための仕組みを提案する．また，システム管理者やグループ管理者の管理の負担を削減し，コストを抑えつつ実用的かつ安全な仕組みとすることを設計の目標とする．

なお，提案する仕組みでは，Grouper などで実装されている一般的な機能に対しては同機能として取り入れるが，本論文で詳細を述べることは省略する．また，グループを用いて認可を行う際には，各サービス側でアクセスを許可するグループとそれに対するアクセス範囲の指定を行うが，本論文ではグループ管理の仕組みを提案することより，各サービス側で行うアクセス許可の設定については省略する．

4.3.1 前提条件と要件

本研究で提案する仕組みは，以下のような組織で利用することを前提とする．

- 分散管理組織で統合認証基盤が整備されている
- 中央の認証サーバには，在籍者の統合 ID や共通に定義される属性が格納されている
- 中央の認証サーバのユーザ情報は，ユーザごとの管理部局や別に管理されるサーバなどと連携を行い，日々最新の情報に更新されている

グループ管理機能に対する基本的要件は以下とする．

- グループごとにグループ管理者を立て分散的に管理できること
- 統合認証基盤と連携することより，グループ管理者やメンバの指定に，統合 ID や属性を使用できること
- 列挙型，属性型，複合型によりメンバ登録できること

4.3.2 既存のグループ管理の仕組みの課題に対する提案

課題解決のために次の二つの提案を行う．一つは，グループの柔軟性の向上のために，グループ管理者になれる権限を一般ユーザにも拡張し，参照権限を確保しつつ参照権限の範囲外のユーザもメンバにできるようにすることである．このグループを本研究では「一般グループ」と定義する．もう一つは，グループの必要に応じて継続性を確保するため，業務などで使用するグループで継続性が必要とされるグループを「公式グループ」と定義し，システム管理者がグループ管理者の管理を行う．グループ管理者の交替がスムーズに行えるよう，グループ管理者を属性でも指定可能とする．

一般的にグループ管理に必要とする操作は，図 4-1 のとおり，グループ管理者になる人の申請から始まり，システム管理者による申請内容の確認後，グループ管理者の登録，参照権限の設定が行われ，設定完了後にグループ管理者によるグループの登録，グループ管理者の追加，メンバ登録という流れになる．参照権限を越えたユーザを追加する際や，削除になったグループを復活する際などの個別対応が必要な場合は，都度，グループ管理者が個別対応の申請を行い，システム管理者が個別設定を行うなど，非常に多くの手順が必要になる．これらの操作手順は，本提案の仕組みを導入することにより，大幅に削減される．

以下に提案について詳細について述べる．

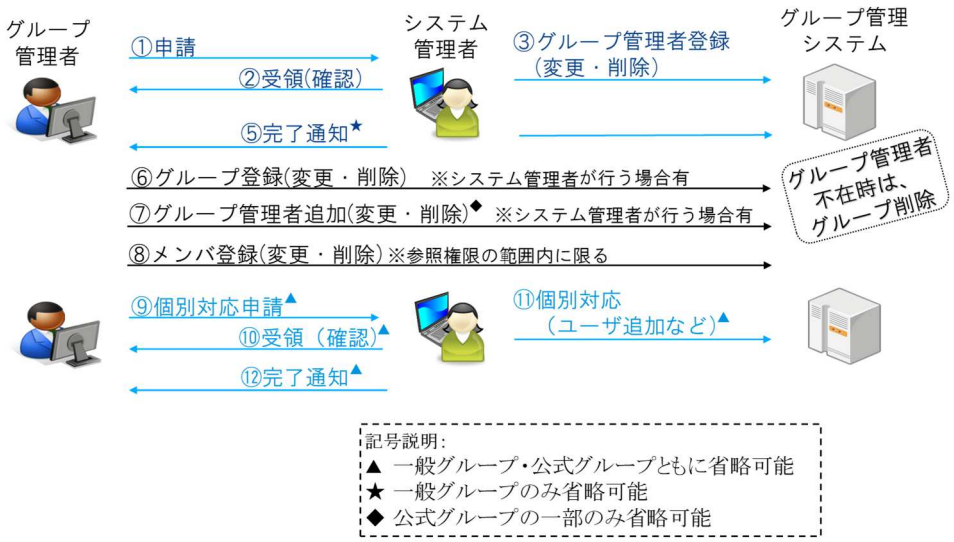

図 4 - 1　一般的なグループ管理の操作

4.3.3 グループの柔軟性の向上

4.2 節で述べたように，これまではシステム管理者がグループ管理者を登録しグループ管理者ごとに設定された参照権限の範囲内でしかグループのメンバ登録ができなかったのに対し，本研究では，グループ管理の権限を特定のユーザだけではなく一般のユーザにも移譲することでグループの柔軟性を拡張する．その際にグループ管理者は与えられた参照権限を保持しつつ，参照権限にとらわれない柔軟なメンバ構成のグループが作成できる仕組みを提案する．本研究では，一般ユーザが自由に作成できるグループを「一般グループ」として扱う．

以下，グループ管理者に参照権限が与えられていないユーザをメンバとして登録する際

の具体的な操作を述べる．列挙型ではメンバにしたいユーザの ID を登録する．ユーザの ID が不明な場合は直接ユーザに問い合わせるなど行うことで ID を登録する．属性型では，属性に対する条件式によりメンバを導く．属性型のグループは，ユーザの属性が変更されれば，グループに含まれるメンバは設定値に合わせて自動で変更される．複合型は，自身がグループ管理者になっている既存のグループ，もしくはグループの存在を公開しているグループを組み合せることでメンバを導く．既存のグループのメンバが変更になれば，それに合わせて自動的にメンバが変更される．ただし，属性型のグループも複合型のグループも導かれたメンバリストは参照不可とする．個人情報保護などの要請により，ユーザ担当掛などである場合を除き，一般ユーザは，同組織内であっても所属や身分が異なる人の在籍情報を知ることができない場合が多くなっている．グループのメンバかどうかが判ればそのユーザの属性値が判ってしまうことから，原則，一般グループのグループ管理者は，条件式から導かれたグループのメンバリストに加え，メンバ数も閲覧不可とする．メンバリストの閲覧ができない場合，属性情報が想定するものと異なることや条件式の誤りなどにより，グループ管理者の意図しないメンバ構成になることが考えられる．しかし，Web サービスのアクセス制限において，認証サーバに格納されているユーザの属性を直接指定して認可の判断を行う場合，認可の条件に該当するユーザのリストを直接閲覧することはできず，その該当の属性を持つユーザであれば，そのサービスにアクセスすることができるようになる．これと同様に，本研究におけるグループにおいても，Web サービスのアクセス制限などの利用を前提とすることより，原則，作成したグループのユーザリストはグループ管理者が閲覧できない運用とする（図 4-2）．

これらより，一般グループでは，これまでの仕組みでは実現されなかった一般ユーザが参照権限を越えた学科や学部を横断したグループや，複数の研究室を合わせたグループの作成が可能になる．作成されたグループは，掲示板などのサービスやスケジュール管理などのサービス，メーリングリストなどのサービスと連携することで利用可能となる．安否確認サービスなどでグループのメンバ情報のみ確認するということも，技術的には可能になる．ただし，メーリングリストにグループを使用する際，属性型や複合型の場合には，転送先のリストが不明である場合や，受信を希望しないメンバが副余れている可能性もあるため，公式グループに限定するなど，厳格なルール作りが必要になると考える．

各サービス側で，グループを用いたアクセス制限の設定を行う際，条件式から導かれたグループのメンバが参照できないことにより，意図しないメンバが含まれている可能性も考えられる．取扱注意の重要情報サイトへのアクセスや，全てのリソースにアクセスするような重要なアクセス権限にグループを使用する場合，メンバを確認できる必要があるこ

とより，メンバの閲覧が可能な列挙型のグループにするか，属性型や複合型の場合は 3.2.2 節で記す公式グループとして作成し，その該当グループを指定するのがよい．公式グループでは，グループ管理者はメンバリストを確認できるため，アクセスすることを許さない人がそのグループに含まれていないかを確認しつつメンバの調整を行うことができる．

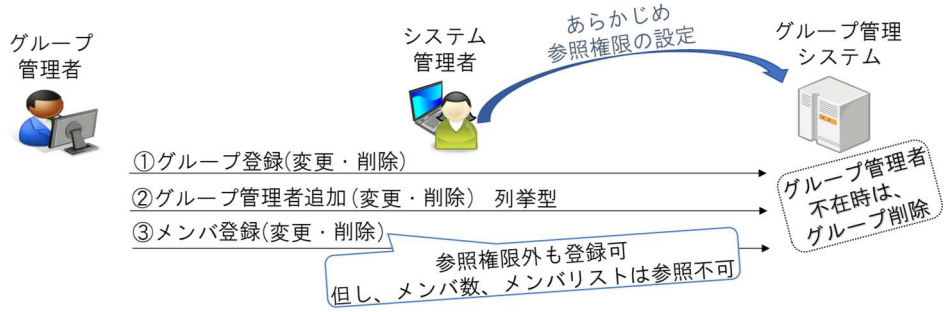

図 4‐2　一般グループに必要な操作

参照権限の設定は，システム管理者があらかじめ，ユーザごとに割当てられた身分や所属などの共通の属性に対して，条件式を設定しておくことで，これにより，新規ユーザの追加時やユーザの所属や身分などの属性値の変更時に，都度グループ管理者の参照権限の設定変更を行うことの負担を軽減する．なお，条件式は，運用方針の変更時や組織改編などにより属性や属性値の構成変更時には変更が発生するが，日常的に変更されることを想定しないものとする．

また，分散管理組織では，教職員と学生，外部組織に所属する研究者など様々な身分により構成されるため，一般ユーザとなる在籍者全員にグループ管理者になれる権限を与えると責任問題に発展する可能性が高まることより，グループ管理者になれる権限を常勤教職員のみに限定するなど，システム管理者があらかじめ認証サーバで共通に定義される属性を用いて制限を行う．

4.3.4 グループの必要性に応じた継続性の確保

これまでのグループ管理の仕組みでは，グループが公式なものであるか，重要なものであるかなどを区別せずに管理されてきたのに対し，本研究では，グループの重要度に合わせて，業務などで使用し，継続が必要なグループを「公式グループ」として定義づける．

公式グループでは，グループ管理者が不在になってもグループが継続できるよう，シス

テム管理者がグループおよびグループ管理者の管理を行う．グループ管理者は，システム管理者から権限移譲された人に限定し，指定されたグループに対してメンバ管理のみ行う．公式グループでは，業務などで使用するグループにおいて意図しないメンバ構成とならないようにすべきであるため，例外的に属性型や複合型から導かれたメンバリストの参照を可能とする．

業務などで使用するグループの管理者は，役職や掛などで決められている場合が多い．これまでのグループ管理システムでは，グループ管理者として個人を登録していたが，個人が人事異動しても，グループの継続は必要であり，異動の度に該当するグループのグループ管理者を変更操作することは，システム管理者の負担が非常に高く，登録・削除漏れが発生する可能性も上がる．

そこで，公式グループのグループ管理者の登録には，異動時などにおける対応作業の効率化のため，グループ管理者として個人の登録だけではなく，ユーザ属性を用いた条件式から導ける仕組みを提案する（図 4-3）．これにより，グループ管理者から新グループ管理者へスムーズな権限移譲を実現し，運用コストの削減にもつながる．

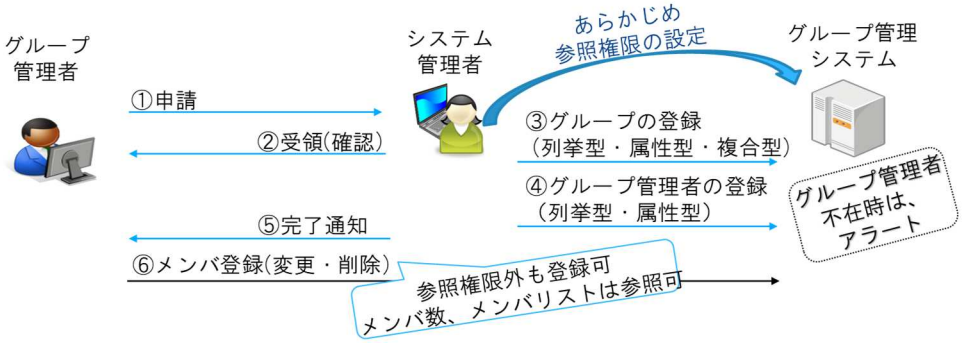

図 4 - 3　公式グループに必要な操作

なお，一般グループにおけるグループ管理者の追加は，これまでのグループ管理の仕組みと同様，グループ管理者を個々に列挙することで行う．グループ管理者の集合が空になったグループは，一定期間後削除する．

提案する公式グループと一般グループに関する相違点を，表 4-3 にまとめる．また，公式グループと一般グループの概要図を図 4-4 と図 4-5 にまとめる．

表 4 - 3　提案する公式グループと一般グループ

	公式グループ	一般グループ
グループの作成者	システム管理者	一般ユーザ
グループ管理者の登録者	システム管理者	グループ管理者
グループ管理者の登録方法	個々に列挙，属性を指定 既存公式グループを指定	個々に列挙
メンバの管理者	グループ管理者	グループ管理者
グループ管理者不在時のグループの操作	継続（システム管理者にアラート）	削除

運用上，公式グループか一般グループかの判断は，組織ごとに重要性と継続性の確保がどれくらい求められているかにより決定するものとする．グループとしては重要であっても，例えば，使用期間が 10 日間であるグループは，その間にグループ管理者が変わらない可能性が高いため，公式グループでなくてもよい．一方，ほとんど使用しないグループであるが，10 年間継続しなければないグループは，継続期間中にグループ管理者の交替が発生する可能性が高く，その際にグループ管理者が不在時になる可能性も考えられる．このようなグループにおいては，公式グループとする方がよいと考える．グループは 1 年間以上継続される場合，グループ管理者が交替されることを考えた方がよく，その際に継続性の確保が必要な場合は，公式グループとして扱う方がよい．

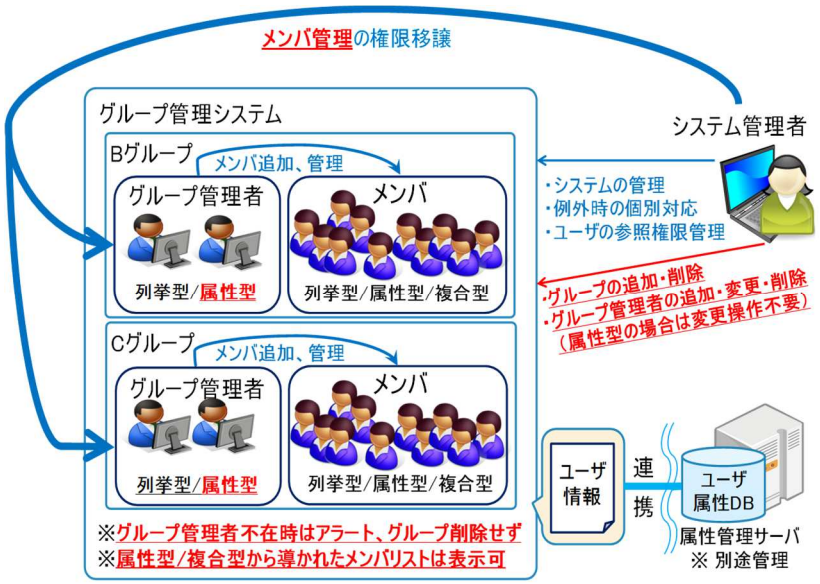

図 4 - 4　公式グループの概要

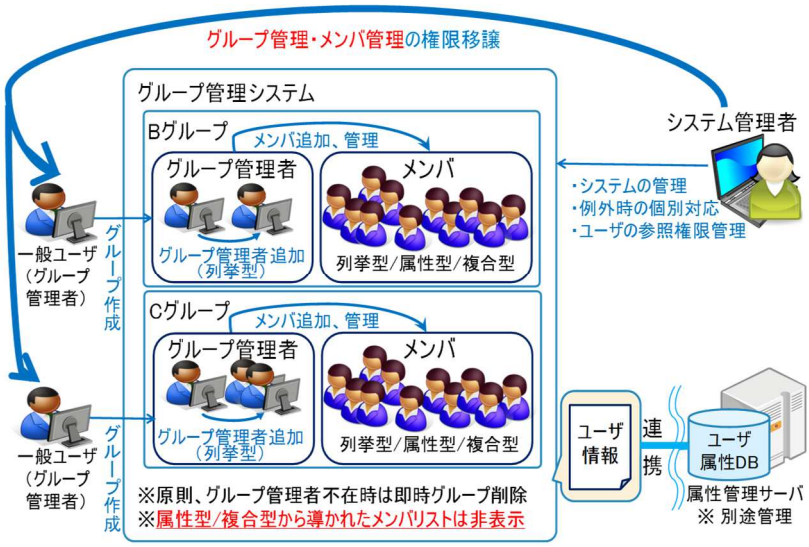

図 4 - 5　一般グループの概要

4.3.5 提案の仕組み導入により軽減される操作

提案の仕組みを用いることで，一般グループでは，あらかじめ一般ユーザに参照権限を設定しておくことで，グループ管理者は，申請不要で自由にグループが作成できるようになり，グループ管理者とシステム管理者間における申請や登録などの操作（図 4-1 の手順 1～5）が削減する．そして，グループ管理者は参照権限にとらわれない柔軟なメンバ構成のグループが作成できるようになることより，グループ管理者の参照権限を越えたユーザをメンバに追加するなどの個別対応が必要な場合の操作（図 4-1 の手順 9～12）も削減になる．

公式グループでは，システム管理者がグループ管理者およびグループの管理を行うことより，申請や登録などの操作（図 4-1 の手順 1～3,5）は削減できないが，一般グループと同様，あらかじめ一般ユーザに参照権限を設定しておくことにより，グループ管理者ごとの参照権限の設定（図 4-1 の手順 4）と，それに伴う個別対応（図 4-1 の手順 9～12）が削減になる．公式グループでは，グループの登録（図 4-1 の手順 6）や，グループ管理者の追加（図 4-1 の手順 7）はシステム管理者が行う．グループ管理者の追加においては，公式グループでは，グループ管理者を属性型により指定する場合は，ユーザの属性変更に合わせてグループ管理者も自動で変更されることより，この操作（図 4-1 の手順 7）も削減になる．

これらの操作が発生する頻度について，次に述べる．頻度を算定するに当たっては，

5000 人規模の組織を前提とする．グループ管理者の登録は，連携するサービスの追加などに合わせてグループの作成が必要になる都度発生する．連携するサービスの追加は，1 年間で約 5 件，1 つのサービスにつき作成が必要となるグループ数を 10 グループと想定した場合，1 年間で約 50 グループに対するグループ管理者の登録が必要になる．グループ管理者は，作業効率や責任問題などより，同じ人が一定期間は継続すると考えられるため，グループ管理者の交代は 1 グループにつき 3 年に 1 度程度発生すると想定する．これは 1 年間においては，存在するグループの約 1/3 のグループに対するグループ管理者の変更が必要であることになる．これらを元に算定すると，グループ管理者の登録と変更に係る操作は 1 年間において，70 回程度発生すると想定される．本提案の仕組みを導入することで，上記の削減された多くの操作に対して，1 年間で約 70 回分削減されることになり，グループ管理者およびシステム管理者の負担が大幅に削減されることが期待できる．

これらを具体的な数値で表すと，1 回あたりの操作に申請，登録作業，承認，管理，ダブルチェックなどが必要となることより，1 回あたりの作業工程を 2 人日，1 人日あたりのコストを 10,000 円と想定すると，グループの管理者の新規登録や変更は 1 件につき 20,000 円のコストが発生することになる．1 年間においてグループの 70 回程度発生すると想定すると，1,400,000 円のコストが必要になる．

4.3.6 提案するグループ管理システムの設計

提案するグループ管理システムを実現するためには，グループやユーザに関するデータの格納が必要であることより，データベース構造を用いる．グループ管理システムには，グループを作成し操作するためのルールや参照権限などのルール，ユーザがアクセスする際のインターフェースなどの他，作成したグループに関するグループテーブル，メンバを登録するための元となるユーザ属性テーブルをデータベースとして管理する．ユーザ属性テーブルには，氏名，統合 ID，所属，身分など共通に定義された属性を格納する．格納する情報は，中央でユーザ属性を管理する認証サーバなどと常に連携することで，最新の状態に保つ．中央のサーバに格納されていない兼務などの情報をユーザ属性テーブルに格納したい場合は，別途，他部局で管理されるサーバと連携するか，システム管理者が他部局からデータを受領し，直接ユーザ属性テーブルに追加する．グループテーブルには，作成されたグループ ID やグループ管理者，メンバ，グループの種類などを格納する．グループテーブルの情報は，ユーザ属性テーブルのユーザ属性の変更が発生すると，属性型や複合型により作成されたグループのメンバリストも更新する．

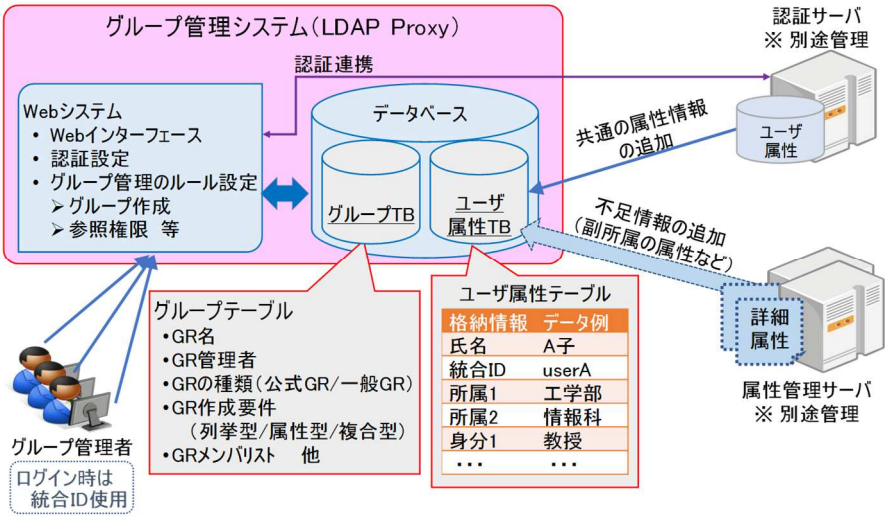

図 4 - 6　提案するグループ管理システムの概要

グループ管理者が操作するための Web インターフェースを用意し，ログインする時には，各ユーザの統合 ID にてログインできるよう，別途中央で管理されている認証サーバと連携する. 参照権限の条件式は属性と属性値に対してあらかじめ作成しておくものであり，常に変更が発生するものではないため，Perl スクリプトなどで自由に記述できるようにしておく（図 4-6）.

4.3.7 グループ管理システムにおけるグループ管理に必要な操作

（１）グループに対する操作

グループに対する操作は，大きく以下の 3 つに分けることができる.

グループに対する操作：

A)　グループの作成

B)　グループへのメンバの追加/削除

C)　グループの削除

B)は，列挙型の場合，個々のグループ管理者が，必要に応じてユーザの追加や削除を行うこととなる．属性ベースで定義されたグループは，初回のメンバ登録時だけでなく，変更や削除時においても，グループ管理者が操作しなくても，条件式に合わせて常に最新の

メンバ構成になっていることが必要である．

（２）グループ参照時の操作

グループ管理を実現する際に，属性ベースで定義されたグループは，ユーザの属性の変更に応じて，メンバが変更になる．そのため，常に最新のメンバ情報を得るためには，グループごとにメンバを格納するのではなく，問い合わせがある度にメンバが展開されることが望まれる．

しかし，本研究で管理するグループは，各サービスからの認可だけではなく，メールエイリアスなどでも応用できることとするため，グループのメンバリストが常に必要される．また，与えられたユーザが指定されたグループのメンバか否かの判定やグループのメンバの人数の参照をスムーズに行うことが必要だと考える．まとめると，グループの参照時に必要な操作は以下のようになる．

グループの参照時に必要な操作：

- **ユーザのグループメンバーシップの参照**
  （与えられたユーザが指定されたグループのメンバか否かを YES/NO で判定するため）
- **グループのメンバリストの参照**
  （与えられたグループのメンバのリストを得ることができるか）
- **グループのメンバ数の参照（あるいは空グループか否かの参照）**

ここでは，これらに対して，それぞれ属性などの変更によりメンバが更新される頻度と，それに対してどれくらいリアルタイム性を求めるか，ということが検討課題となる．

（３）グループ管理の操作

本研究では，ユーザ属性は，別途ユーザ属性を管理するサーバと同期するが，ユーザ属性の変更は 1 日に何度も行われないことより，全グループのメンバリストの更新は，1 日 1 度行えばよいと考える．ただし，ユーザ属性の変更によりアクセス制限の許可がされなくなったユーザが約 1 日の間，利用できることは，アクセス制限のセキュリティ面の観点から考えると好ましくない．そのため，ユーザ属性の変更により，グループのメンバではなくなる場合に限り，メンバリストから即時削除することとする．

具体的な動きは，グループ管理システムのユーザ属性 DB には，ユーザ属性を管理するサーバから得る情報だけでなく，所属するグループの情報も格納する．それにより，ユー

ザ属性の変更時，参加するグループの条件式を確認し，条件に当てはまらなくなった場合は，グループのメンバリストから削除する．これにより，サービスの認可でアクセスを許可する場合に，不要なユーザの利用を避けることができる．さらに，ユーザ属性 DB に所属するグループ情報を格納することで，与えられたユーザが指定されたグループのメンバか否かを即時に知ることができ，利便性の向上につながる（図 4-7，図 4-8）．

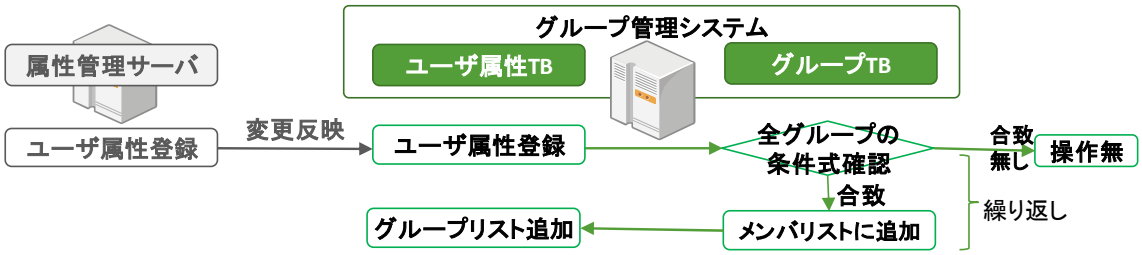

図 4 - 7　ユーザ属性登録時の流れ

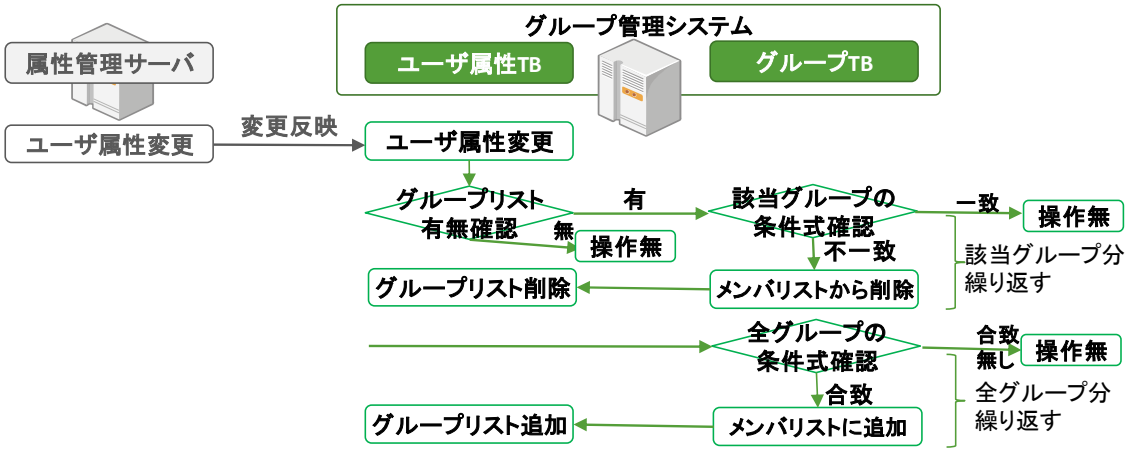

図 4 - 8　ユーザ属性変更時の流れ

4.4 提案するグループ管理システムの実装

本章では，4.3 節で提案する仕組みを元に実装したグループ管理システムについて述べる．実装するグループ管理システムは，Grouper などで用いられている一般的な機能を取り入れつつ構築を行った．

4.4.1 実装するグループ管理システムの概要

作成したグループは Web サービスなどの認可に使用するため，認証サーバである LDAP サーバのプロキシサーバになるよう LDAP Proxy 機能を用いて統合グループ管理システムとして構築し，その上でグループ管理システムを実現した[97][98]．実現する際の OS は CentOS 6.4，LDAP Proxy 機能の実現には openLDAP2.4.23，言語には Perl 5.10.1 を用いた．データベースには MySQL 5.1.73 を用いた．

グループ管理者が操作するための Web インターフェースには，Apache 2.2.15 を用いた[99]. Web インターフェースにログインする時には, 統合 ID にてログインできるよう，別途，中央で管理されている LDAP サーバと連携を行った（図 4-9）．Web インターフェースを構成する HTML の版は，クライアント側で動的な処理を想定していないことと，試験稼働のためアクセス範囲を学内限定とし，学内の PC からの利用を想定していたため，HTML4.01 とした．Web インターフェースへのアクセスは，スマートフォンからの利用時には，PC 用の画面として表示されるが利用は可能である．

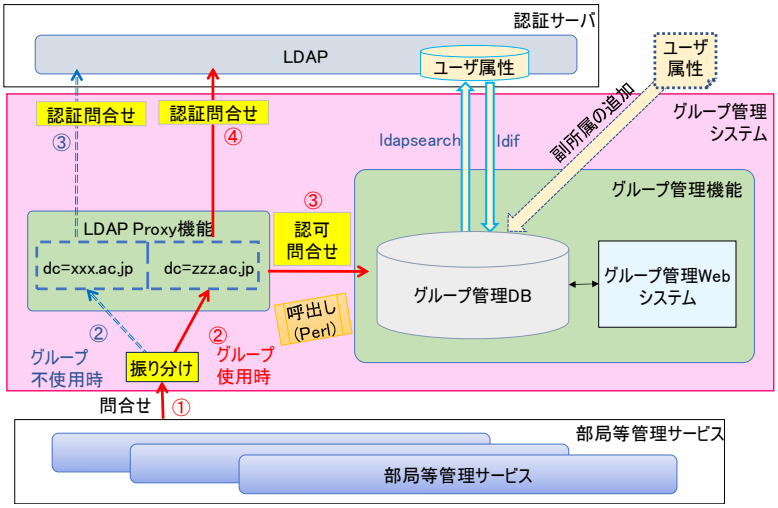

図 4 - 9　実装するグループ管理システムの全体構成

（1）　インジェクション対策

提案の仕組みの実装では，Web インターフェース上でテキストを入力することより，悪意のある利用者が Perl スクリプトを使ってシステムを攻撃することも想定される．そのために，インジェクション対策が必要となる．試験運用期間は，アクセス可能な範囲を学内限定としていたことより，以下の対策を行った．

・入力文字数の制限

・quote 関数を用いたエスケープ処理

本格運用する際には，オープンソースの WAF（Web Application Firewall）である ModSecurity などの導入が必要であると考える．

4.4.2 グループの操作

グループに対する操作は 4.3.5（１）で述べた A)グループの作成，B)グループへのメンバの追加/削除，C)グループの削除の流れになる．

（1） グループの作成

一般グループでは，グループを作成したい一般ユーザが，自身の統合 ID とパスワードでグループ管理システムにログインし，グループ ID や用途などの必要情報を入力することでグループの作成を行う．グループ作成を行ったユーザはグループ管理者となり，必要に応じてグループ管理者の追加を行う．公式グループでは，システム管理者がグループ管理システムにログインし，グループとグループ管理者の登録を行う．グループ管理者は列挙型もしくは属性型，複合型により登録を行う．

（2） グループへのメンバの追加/削除

グループ管理者に参照権限が与えられていないユーザをメンバとして登録する具体的な方法について，列挙型，属性型，複合型のそれぞれに分けて以下に述べる．

列挙型では，グループ管理者がメンバにしたいユーザの ID を直接入力し，メンバ追加をする．ユーザの ID が不明な場合はユーザに直接問い合わせなど行うことで ID を登録する．属性型では，属性に対する条件式を入力する事で，メンバを導く．複合型は，自身がグループ管理者になっている既存のグループ，もしくはグループの存在を公開しているグループを組み合せることでメンバを導く．属性型と同じく，原則，導かれたメンバリストの閲覧，導かれたメンバ数の閲覧も不可とする．ただし，属性型と複合型のいずれの場合も，グループ管理者毎に設定された参照権限により，作成されたグループの全メンバがそのグループ管理者の参照権限の範囲内に含まれるユーザである場合には，メンバリストの閲覧を許可する．

なお，ユーザの属性変更は，日々の頻度が低く毎日頻繁に行われるわけではないことより，試験運用では，ユーザ属性テーブルの更新は 1 日 1 回とし，ユーザ属性テーブルの更

新に応じて, グループテーブルに格納されているメンバの情報を更新する仕組みとしている.

(3) グループの削除

実装したグループ管理システムでは, 一般グループでは, ユーザ属性テーブルからグループ管理者になっているユーザが全員削除された時点で, そのグループは削除される. 公式グループでは, グループ管理者が不在時になって時点でシステム管理者にアラートを挙げるが, 即時にグループを削除することは無く, システム管理者が随時必要に応じて削除を行う.

4.4.3 参照権限の条件式

参照権限の条件式は Perl スクリプトで自由に記述できるようにしており, Perl の正規表現などを用いることも可能である. 記述箇所は, Web インターフェース上ではなく, プログラム内の指定した箇所とした. 3.2.1 の後ろから 2 段落目のとおり, 条件式は日常的に変更されることを想定していないものであるためである.

条件式は, 参照する人と参照される人のそれぞれに割当てられている身分や所属などの指定された属性に対して, 属性値が一致する場合や属性値が特定の値である場合に参照可となることを, 関係演算子（＝, ＜, ＞等）を用いて記述する. 複数の属性値を組み合わせる場合は, 論理演算子∧(and), ∨(or)と￢(not) を用い, 条件式を複数設定することで, それらのいずれかが成り立てば参照可とする.

例えば, 一緒に業務を行うような同じ身分かつ同じ所属の人に対する場合や教員が担当するゼミを受講する学生に対する場合, 大学院掛が大学院生に対する場合など, 一般的に参照を許可してよい範囲に対して参照権限を与える条件式を設定する. これらの例を条件式で表すと以下になる.

条件式の例：

$x.a$ = "職員" ∧ $y.a = x.a$ ∧ $y.b = x.b$ (1)

$x.a$ = "教員" ∧ $y.a$ = "学生" ∧ $y.c = x.c$ (2)

$x.b$ = "大学院掛" ∧ $y.a$ = "学生" ∧ $y.d \geqq 5$ (3)

x：参照する人（グループ管理者）

y：参照される人（ユーザ）

$x.a$：属性値（a：身分　b：所属　c：担当ゼミ名/受講ゼミ名　d：勤続年数/学年）

条件式では，X を参照する人の集合，Y を参照される人の集合，その要素をそれぞれ x, y とする．ここでは，説明を簡単にするために参照権限に利用する属性値の成分を a:身分，b:所属，c:担当ゼミ名もしくは受講ゼミ名，d:を勤続年数もしくは学年とする．使用する属性は一般ユーザに割当てられた共通のものとする．

条件式(1)は，グループ管理者 x の身分属性の値が職員であれば，身分属性と所属属性の値が同じユーザに参照権限を与えるという式である．条件式(2)では，グループ管理者 x の身分属性の値が教員，ユーザの身分属性の値が学生であり，グループ管理者の担当ゼミとユーザの受講ゼミが同じ場合に参照権限を与える．条件式(3)の場合は，グループ管理者 x の所属属性の値が大学院掛であり，ユーザの身分属性の値が学生であり学年が 5 以上（大学院生）の人に参照権限を与える．試験運用時では，参照権限の条件式は，参照する人の身分属性が教職員であり，参照する人と参照される人の詳細な所属属性の値が同じ場合のみとした．

また，試験運用においては，一般グループのグループ管理者になれるユーザは，常勤教職員の属性を保持しているユーザのみとした．

4.4.4 各サービスとの連携

本研究で構築したグループ管理システムは，将来的に統合認証基盤と連携する全てのサービスからの認証認可の窓口となれるよう，認可にグループを使用しない場合でも経由できるよう LDAP Proxy 機能を用いた仕組みとした．

各サービスからグループを用いて認証認可を行う際，認証認可の流れは，ユーザが各サービスにアクセスした後，各サービスから LDAP Proxy 機能に対して問合せを行い，グループを使用するか否かの判別を行う．グループを使用する際には，グループ管理機能に対して該当ユーザが該当のグループに属するか否かの認可問い合わせを行う．認可問合せに成功すれば，認証サーバである LDAP へ認証問合せを行う．認可にグループを使用しない場合は，LDAP Proxy 機能から LDAP へ認証問合せを行う．

なお，各サービス側において，認証認可問合せを LDAP Proxy に向けて行うことと，アクセス範囲とアクセスを許可するグループの設定をすることが必要であるが，3 章のとおり，本論文では省略する．

4.5 グループ管理システムの試験運用と評価

4.5.1 グループ管理システムの試験運用

実装したグループ管理システムは，2013 年 5 月より約 3 年間，東京海洋大学品川キャンパス内にて試験運用を行った．グループは資産を管理するためのシステムや，ユーザを限定する Web ページへのアクセスなどの各サービスの認可ユーザとして使用された．グループ管理システムには，多い時には約 150 のグループがあり，公式グループが約 100，一般グループが約 50 存在した．それぞれのグループのメンバ数は，平均して 1 グループにつき 10 名から 20 名程度登録されていた．グループ管理システムにアクセスできる人は身分属性が教員か職員とした．

公式グループはグループ管理者になる人の申請により，システム管理者がグループとグループ管理者を登録する運用とした．公式グループの用途は，研究室などの小単位で管理されているネットワーク機器情報等の資産を管理するシステムへのアクセス制限などで利用された．研究室などの小単位ごとに資産の管理責任者となっている人をグループ管理者とし，グループ管理者は実務担当者をメンバとして登録した．研究室では教員が，部や課では部長や課長がグループ管理者となり，メンバには，グループ管理者の参照権限の範囲を越えた秘書や大学院生，非常勤職員なども登録された．グループ管理者が所属や役職により決められる場合は，該当の所属属性や役職属性を指定した．

一般グループの多くは，授業やゼミ，委員会などの単位で利用する Web サービスへのアクセス制限などに用いられた．各 Web サービスの管理者などがグループ管理者となり，アクセス可能なユーザをメンバとして登録する．参照権限が無く ID が不明なユーザに対しては，授業などで ID を確認しつつ個々に ID の追加を行っていた．

試験運用では，公式グループのグループ管理者においては，属性を指定していたグループが約 10 分の 1 にとどまり，多くのグループが個々に ID を登録していた．その理由として，属性を指定する際に用いる別途中央で管理する認証サーバ上の属性情報が，公式グループの管理者を特定するには詳細さや正確さが足りなかったことが挙げられる．例えば「所属」属性に対しては，部，課，掛など階層が異なる情報が格納されていることや，何も格納されていない場合があること，変更が即時に反映されないことなど，属性情報の管理が十分になされていなかった．そのためグループ管理者には個別に ID を登録することとなり，グループ管理者の変更時にシステム管理者の操作が発生するケースもあった．また，このような中でグループ管理者が異動などで不在になり，グループ管理者の再設定を

行ったグループが 3 件あった.

4.5.2 試験運用の評価

実装したグループ管理システムは，試験運用の 3 年間において，大きなシステムのトラブルはなく，運用ではシステム管理者の個別対応も対応可能な想定の範囲で行われた.

本グループ管理システムを用いることで，一般グループでは，システム管理者があらかじめユーザ属性ごとにグループ管理者の参照権限を条件式として設定しておくことで，一般ユーザがシステム管理者との間で複雑な手続きを交わすことなくグループ管理者になれるようになり，グループ作成におけるシステム管理者とグループ管理者の管理の負担が軽減された．また，グループ管理者の参照権限の範囲を越えたユーザをメンバにできることより，システム管理者が個別対応を行うことなく，一般ユーザが教員と学生が混在する研究室用や授業履修者用などの希望するグループを自由に作成できるようになった. 公式グループでは，グループ管理者に属性から導くことで，グループ管理者の変更時に変更申請などの手続きを行わなくても新グループ管理者へスムーズに変更ができるようになり，システム管理者に対するグループ管理者の管理の負担が軽減された.

試験運用を行った 3 年間においては，一般グループでは，管理者登録に関する操作（図 4-1 の操作 1,2,3,4,5）と，個別対応に関する操作（図 4-1 の操作 9,10,11,12）の 9 つの操作を約 50 回分削減された．公式グループでは，参照権限の設定に関する操作（図 4-1 の操作 4）と，公式グループの一部における一部グループ管理者変更時の操作（図 4-1 の操作 7）と，個別対応に関する操作（図 4-1 の操作 9～12）の 6 つの操作が約 100 回分削減された．また，権限移譲においては，システム管理者からグループ管理者へ権限移譲されたグループ管理者の管理権限は，一般グループとして作成されたグループ数に値する約 50 件，グループ管理（メンバ管理）の権限は，一般グループと公式グループの両グループ数に値する約 150 件であった. グループ管理者から新グループ管理者への権限移譲は，属性を指定する際に用いる別途中央で管理する認証サーバ上の属性情報が，公式グループの管理者を特定するには詳細さや正確さが足りなかったことより，グループ管理者に属性を指定することができた約 10 件であった.

これらより，提案するグループ管理システムを用いることで，システム管理者からグループ管理者へ，グループ管理者から新グループ管理者へ権限移譲が効率的に行われるようになり，また，システム管理者とグループ管理者のグループ管理に対する負担が軽減され，運用コストの削減にも繋がったことが確認できた.

試験運用では，グループ管理者になれる権限をトラブルがあった際の責任問題を考え常勤教職員のみに限定した．また，公式グループか一般グループかの判断においては，連携するサービスが業務として複数年間提供されることが確定している場合に，そのサービスへアクセス制限などとして利用するグループに対して，公式グループとして扱った．この 2 点はシステムに実装されていない運用上のノウハウである．このような知見は，このシステムの利用者間で共有していくことが有用であると考える．

一方，3 年間の運用において，提案する仕組みを効果的に働かせるためには，次の課題があることも明らかになった．課題の一つ目は，提案する仕組みでは，属性の管理において， 属性の設計がグループの作成を意識したものになっていることと，属性の情報が遅滞なく反映されていることの 2 点が前提となっていることである．しかし，実際の大学などの分散管理組織における現状では必ずしもそうはなっていないため，本提案の仕組みを効果的に使うためには，中央の認証サーバが更新される時期と合わせて属性の構成の見直しと属性の正しい管理体制を整えることが必要である． 正しい属性情報が登録されることにより，システム管理者やグループ管理者の交替時の操作およびそれに伴う手続きが省略できるようになるため，さらなる運用コストの削減が期待できる．

課題の二つ目は，試験運用したシステムでは一般グループから公式グループへの移行のプロセスをサポートできていなかったことである．一般グループから公式グループへの昇格は珍しくないと考えられる事から，容易に移行できる仕組みをシステムが実装していることが運用上望まれる．

試験運用したシステムでは，参照権限を越えた属性型や複合型により導かれたグループのメンバリストを原則として閲覧不可としているが，連携する Web サービスなどから認証認可を行う際には，その Web サービスの管理者はアクセスしたユーザ情報を知ることができることが判明している．これが運用上，認められない場合には，Shibboleth 等のプライバシーに配慮した認証連携の仕組みを取り入れていく必要がある．これについては，必要に応じて検討していく予定である．

4.6 結語

本論文では，統合認証基盤が整備されている分散管理組織において，グループ機能を用いて認可情報を統合的に管理する際，既に開発されている Grouper などのグループ管理の仕組みの課題に対して，グループを体系的かつ効率的に管理するための仕組みの提案し，提案の方式に基づきグループ管理システムを実装した．実装したグループ管理システムは，

約 3 年間，東京海洋大学において試験的に運用を行い，評価を行った．

提案する仕組みは，これまでのグループ管理の仕組みで課題とされてきたグループに対する柔軟性と継続性に対して，システム管理者からグループ管理者への権限移譲に着目した仕組みである．柔軟性については，一般ユーザが自由にグループを作成できるグループとし，ユーザに対する参照権限の範囲を越えてもメンバを登録できる仕組みとした．このグループを「一般グループ」と呼び，継続性については，グループの重要度に合わせて業務などで継続性の確保が必要なグループを「公式グループ」と定義付けた．公式グループでは，グループ管理者が不在とならないようシステム管理者がグループ管理者の管理を行い，グループ管理者の交替時にスムーズに交替が行えるようグループ管理者はユーザを個々に登録するだけでなく，属性などを用いて管理することも可能とした．

本研究で提案する仕組みを実装し，試験運用を行ったことにより，システム管理者からグループ管理者，グループ管理者から新しいグループ管理者にスムーズな権限移譲ができ，グループの管理における管理の負担が削減され，運用コストの削減につながることが確認された．

本研究で実装したグループ管理システムは，試験運用を行っていく中で，順次，連携するサービスの追加を行い，全学展開できるよう検討中である．

本研究で実装したグループ管理システムは，メンバにできるユーザを組織内のユーザに限定したが，本研究で提案する仕組みの概念は，組織を越えたグループにも対応できるものである．今後，組織を越えたグループにも対応したシステムとしていけるよう検討を進める予定である．

第5章　キャンパスネットワークと機器の管理

5.1 緒言

近年，情報ネットワークにおいては，急増している不正アクセスなどに対して，企業だけではなく大学などの教育研究機関においても，安全性を考慮した仕組みが求められている[100][101]．多くの大学においては，情報ネットワークを利用する際に，認証機能を追加するなどセキュリティや利便性を重視した仕組みが導入されている[102][103][104]．認証方式は，Web ブラウザを用いて認証を行う方式（以下，Web 認証とよぶ），接続機器の MAC アドレスを事前に登録して認証する方式（以下，MAC アドレス認証とよぶ），IEEE802.1X の規格を利用して電子証明書を使用したりユーザ名およびパスワードを入力する方式（以下，802.1x 認証とよぶ）などが存在する．

大学などの組織では，教育研究の自由が認められていることより，企業のように与えられた PC を利用するだけでなく，研究室などの単位で購入したプリンタやネットワークスイッチ，IoT（Internet of things）機器などを自由に接続して利用できるネットワーク環境が必要とされる．一方，インシデント発生時などに即時に対応できるよう，接続機器の厳重な管理も求められる．

大学のキャンパスネットワークにおいては，接続する機器や使用する IP アドレスについては，建物や研究室などの単位で個々に管理が委ねられている場合が多い．そのため，MAC アドレス認証のような厳格な機器の管理が必要とされない環境の場合は，初回の IP アドレス発行時に申請した機器情報のまま機器の変更があっても IP アドレスがそのまま使い続けられるなど，管理が曖昧になりがちである．

これらより，本研究では，大学のネットワーク（有線 LAN）において，統合的な接続機器の管理と安全性を考慮しつつ接続機器の種類にとらわれず，ネットワーク接続時にユーザが操作不要で接続可能となる MAC アドレス認証に着目した．

大学における接続機器の管理は，研究室などの単位でそれぞれ管理されている．その管理に対する責任者は研究室の責任者である教授などが担っているが，実際には教授から移譲された秘書や大学院生が管理している場合も多い．本研究では，これらの実体の管理体制を考慮し，事前の機器情報の登録には 4 章のグループ管理システムと連携し，研究室などごとの単位で実際に機器を管理する人のグループ（以下，機器管理者グループとよぶ）を作り，統一して接続機器情報を管理できる仕組みを提案する．提案の仕組みでは，トラブルの軽減，トラブル時の早期解決のため，IP アドレスと MAC アドレスを関連付けし，接続機器の監視，通報する仕組み（以下，MAC-IP 監視管理システムとよぶ）を取り入れ

た．本研究では，提案の仕組みを実装し，東京海洋大学の品川キャンパスにおいて，2014 年 3 月より 1 研究棟に試験導入し，2015 年 3 月より全研究棟に拡張した．全研究棟への導入時には，不正接続機器の接続状況などの調査を行い，評価を行った．

5.2 キャンパスネットワークの運用に関する関連技術

5.2.1 従来のネットワーク接続機器の管理体制

キャンパスネットワークの管理において，従来は研究室などで PC などのネットワーク接続機器を購入する度に，機器の管理者（以下，機器管理者とよぶ）が紙ベースなどによる申請書に，機器の管理責任者や，使用場所（建物名・部屋番号など），接続機器情報（MAC アドレスなど）などを記入し申請していた．その申請の内容に基づき，IP アドレスを割り当てるポリシーに従って IP アドレスが割り当てられてきた．しかし，紙ベースによる管理では，情報のやりとりに時間が要することや，MAC アドレス認証を取り入れない場合の IP アドレスの使いまわし，不要になった IP アドレスの返却がなされないなど，問題が発生することがあった．

参考まで，紙ベースの申請を行っていた頃の 2013 年 11 月 19 日から 27 日（1 週間）の間，東京海洋大学品川キャンパスにおいて，IP アドレスと登録されている MAC アドレスを調査した結果，申請書どおりに正しく接続している機器は 28%（2327 件中 658 件）であった（図 5-1）．登録情報が曖昧な場合，ネットワークのトラブル発生時にスイッチ上での問題のポートや MAC アドレスの特定はできるが，該当機器を割り出すための有効な手掛かりにならず，トラブル解決に時間を要する場合が多かった．

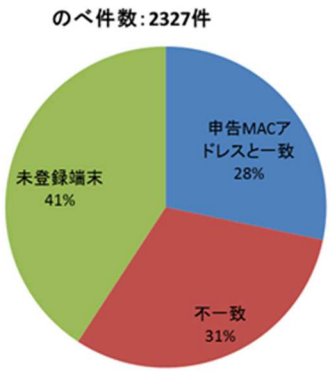

図 5 - 1　IP-MAC アドレス整合性調査結果

（2013/11/19～27，対象エリア：東京海洋大学品川キャンパスネットワーク）

5.2.2 ネットワーク利用時の認証

近年，ネットワークの利用時には，多くの大学において，認証機能を導入し，セキュリティを考慮したシステムが導入されるようになっている．

ネットワーク利用時の認証方式は，Web 認証，MAC アドレス認証，802.1x 認証などが存在する．802.1x 認証の利用は，組織の中央で一元的に管理する機器のみがネットワークを利用する場合などに用いられることが多く，大学においては，ネットワークに接続される機器は，研究室などの単位で様々な機器が導入され管理されるため，組織全体に 802.1x 認証を用いることは難しい．そこで，利用者に対する導入の抵抗や運用のしやすさから Web 認証がよく用いられるが，ネットワークに接続する機器の中には，プリンタ，複合機，IP 電話機など Web 認証が困難な場合も多数存在するため，Web 認証だけでは対応が困難であり，MAC アドレス認証が併用されている大学も多々ある[39][40][105][106]．このように，多くの大学においてネットワーク接続時には認証が採用されている．

Web 認証と MAC アドレス認証のそれぞれの特徴を以下にまとめる（表 5-1）．

表 5 - 1　Web 認証と MAC アドレス認証の特徴

	MAC アドレス認証	Web 認証
管理の対象	機器（MAC アドレス）	ユーザ
接続時の操作	初回のみ MAC アドレスの登録必要	毎回 ID・PW 入力が必要
対応機器	制限無（MAC アドレスさえわかればよい）	ID/PW を入力できる機器からの利用に限定（プリンタ等は不可）
メリット	・ 接続機器の制限が無い ・ 接続都度の認証は不要	・ユーザは機器の登録や申請不要で利用可能 ・認証情報を別途管理の認証サーバ（LDAP サーバなど）と連携すると ID・PW の管理は不要に
デメリット	・ MAC アドレスの偽装ができる ・ MAC アドレスの管理が必要　など	・ ユーザは毎回 ID/PW の入力が必要 ・ ID/PW を乗っ取られると制限なく利用可に ・ ID・PW の管理が必要（LDAP サーバ等と連携する場合は不要）

5.2.3 提案するキャンパスネットワーク管理方式の要件

安全性を考慮した仕組みとするには，厳格な機器の管理だけでなく，管理された機器情報をネットワーク接続時の認証に利用する仕組みも必要である．正しい情報を得るためにも，ネットワーク接続の際の認証システムが必須である[107].

これらを元に，本研究においては，達成すべき目標・前提条件を，次の３つとした．

- 達成すべき目標

I.　セキュリティ強化とネットワーク関連トラブルの迅速な対応と回避策

不正な接続機器の排除と，トラブル発生時に迅速に発生箇所を特定する．リアルタイムの監視を実現して，トラブル発生率削減を目指す．

II.　効率の良い機器の管理（手続き処理の自動化・簡素化）

ネットワークシステムの管理者側・機器管理者側双方の事務手続き・管理業務量を削減あるいは簡素化できるシステムを目指す．

III. 研究室ごとなどの単位での IP アドレスと接続機器の管理

大学などの教育研究機関における各資産の管理は中央で一元管理されるのではなく，各資産の詳細な内容は研究室の中で決められた担当者ごとに管理され，必要に応じて資産ごとに異なる担当部局がとりまとめていることが多い．そのため，各資産を管理するための方式を電子化する際，各資産の担当部局がシステムを管理し，資産の詳細な内容は，研究室ごとの管理担当者が，必要な範囲においてデータを操作できることが望まれる[108][109].

ネットワーク接続機器の管理においても，研究室ごとに機器管理者を設定し，機器管理責任者の裁量で行い，研究室の独自性を重視しつつ，教職員のセキュリティ意識（ネットワーク利用に関する自由と責任の認識）向上に配慮するシステムとすることを目指す．

Ⅲにおける機器管理者は，グループを用いることで，複数名の機器管理者が共通の ID・パスワードを使い回すのを防止するだけでなく，非常勤職員や院生が管理する実情に合わせた形を実現することができる新たな試みとなる．

- 前提条件
  - 機器に対して IP アドレスを固定する
  - 組織内に統合認証基盤システムが導入されている
  - 接続機器は PC だけでなく，共有プリンタ，複合機，IoT 機器等も含む

5.3 MAC-IP 監視管理システムの設計と実装

キャンパスのネットワークにおいて実運用と比較しつつ様々な調査を行った結果, ネットワーク接続機器情報の管理には，各研究室の機器管理者が専用の Web サイトから統合的に管理し, IC アドレスと MAC アドレスによる照合, パケット監視を取り入れた「MAC-IP 監視管理システム」の提案をする．MAC-IP 監視管理システムでは，機器の管理は，研究室などごとに機器管理者を立てて彼らが厳格に管理を行うことで, ネットワークを使用する際の責任者の明確化とトラブル時の早期解決を目指す.

5.3.1 提案する MAC-IP 監視管理システムの設計

MAC-IP 監視管理システムは，ネットワーク監視機能と IP アドレス管理機能により実装する.

ネットワーク監視機能には，大きく以下の 3 つの機能を持つ.

- MAC アドレスの登録
- 未登録機器の検知
- IP アドレスの払出し

接続機器の登録は，IP アドレス管理機能に登録された情報から情報を得て MAC アドレスの登録を行い，MAC アドレスが未登録の機器（以下，未登録機器とよぶ）は，ネットワークに接続できない仕組みとする．IP アドレスの払い出しには，DHCP サーバ機能を用いて IP-MAC 管理テーブルに登録された IP アドレスを払出す機能を提供する.

IP アドレス管理機能では，機器管理者が Web インターフェースにより，IP アドレスの管理や機器情報の登録を行う．機器管理者が IP アドレス管理機能へアクセスする際には，3 章のグループ管理システムと連携し，認証認可を行う（図 5-2）.

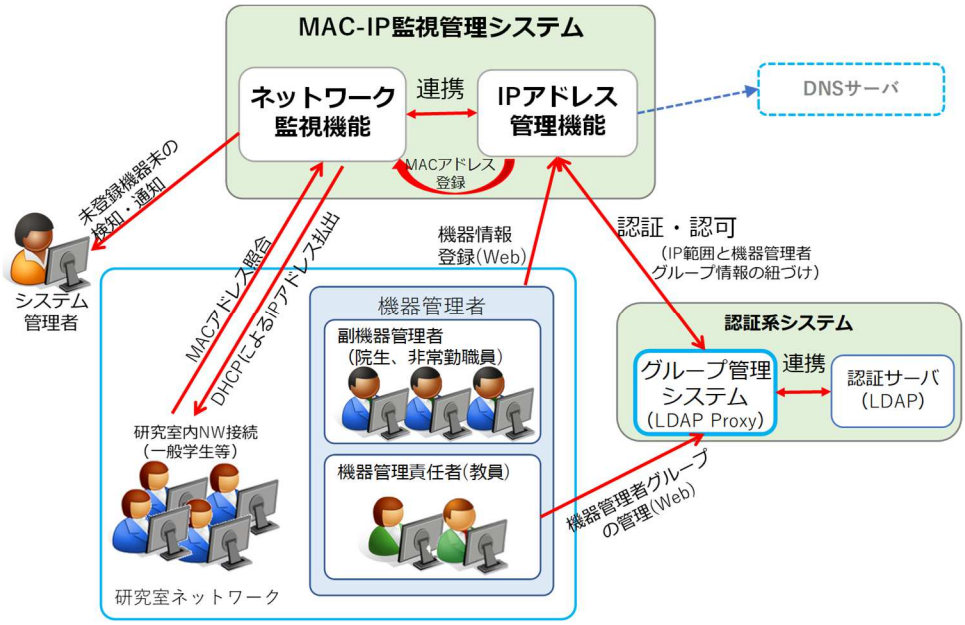

図 5 - 2　MAC-IP 監視管理システムの概要図

IP アドレス管理機能では，格納している IP アドレスや機器情報を csv で出力し，ネットワーク監視機能に送る．また，DNS 連携できるよう DNS サーバにも機器情報を送る．さらに，グループ管理システムと連携することにより，IP アドレスの範囲とグループ情報の紐づけをし，該当グループのメンバが機器管理を行う．

グループ管理システムでは，グループの管理者は，研究室などで機器を管理する責任者責任者である教授などとし，グループのメンバは，機器管理責任者が指名する学生や秘書などとする．グループのメンバに登録されると，機器管理者として，IP アドレス管理機能の操作が行えるようになる．メンバの登録方法は，グループ管理者がグループ管理システムに自身の統合 ID とパスワードでログインし，メンバとして登録したいユーザの ID を追加する．また，グループ管理者である機器管理責任者が退職などにより，不在となる場合は，次に引き継ぐ機器管理責任者の ID をグループ管理者として登録する．グループ管理者は，責任権限のあるユーザであることが必要であるため、グループ管理者になれる人を正規職員などに限定する（図 5-3）．

グループ管理者に統合 ID を用いることより，退職などにより統合 ID が削除されれば，グループ管理者からも削除される．グループ管理システムでは，グループ管理者が不在になり管理されなくなったグループがいつまでも残らないよう，グループ管理者が不在になる場合は，グループは削除となる．グループ管理者を複数名設定している場合，責任権限のあるユーザが不在になれば，残りのグループ管理者にアラートを上げる．しかし，アラ

ート後，一定期間内に，残りのグループ管理者が責任権限のあるユーザをグループ管理者として設定しない場合は，グループは削除となる（4 章参照）．

グループが削除となった場合でも，IP アドレス管理機能とグループ管理機能を切り離して管理していることより，IP アドレス管理機能に登録されている情報は削除されず，これまで登録されている機器は，引き続き使用可能となる．ただし，機器の変更や追加時には，IP アドレス管理機能にログインが必要となるため，再度グループの設定が必要となり，システム管理者が，個別対応を行うことになる．

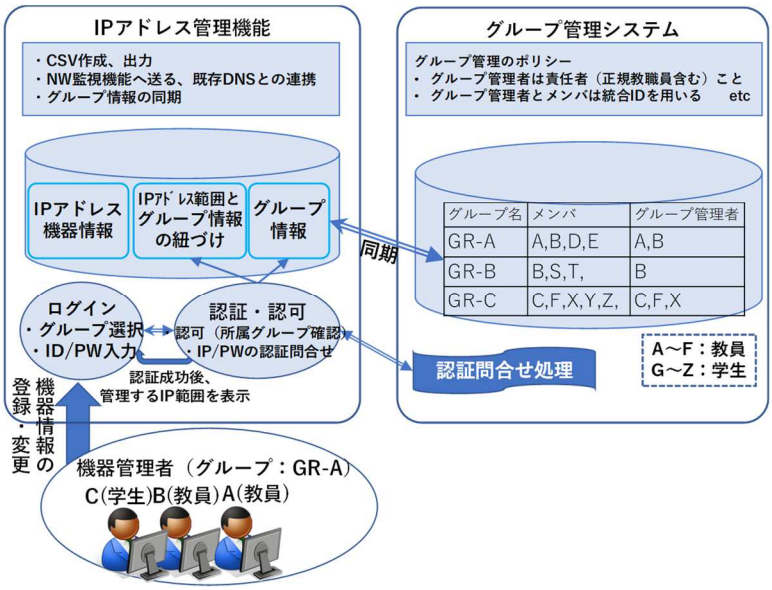

図 5 - 3　IP アドレス管理機能への認証連携の仕組み

5.3.2 実装する MAC-IP 監視管理システムの構成

MAC-IP 監視管理機能システムは，Linux（Red Hat7）上で動作し，ネットワーク監視機能と IP アドレス管理機能を有する．データベースサーバとして PostgreSQL を用いていている．その中で機器管理者テーブル，MAC- IP テーブルなどのテーブルを管理する．

IP アドレス管理機能は，Apache による Web サーバ機能を有しており，システム管理者や機器管理者は Web インターフェースをとおして情報を更新する．システム管理者により，IP アドレス管理機能に，IP アドレスの範囲と機器管理者のグループを割当てることにより，データベース上の機器管理者テーブルにデータが登録される．

IP アドレス管理機能に登録された機器は，データベース上の MAC-IP テーブルに登録され，ネットワーク監視機能により接続可能になる（図 5-4）．

設計では，IP アドレス管理機能は DNS サーバと連携し，登録情報を操作することとしていたが，本研究における実装では，既存のシステムとの兼ね合いの都合上，DNS サーバとは連携せず，IP アドレス管理機能に登録・変更された情報を吐き出すだけとした．

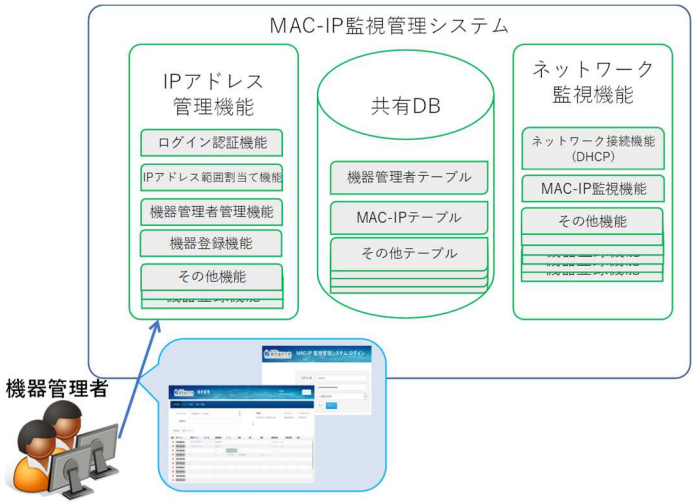

図 5 - 4　MAC-IP 監視管理システム

5.3.3 IP アドレス管理機能とグループ管理システムの連携

IP アドレス管理機能では，IP アドレスの範囲とグループにより認証認可を行う．認証認可のために管理すべき情報はグループとグループに含まれる人が操作する範囲，すなわち IP アドレスの管理範囲のみである．ユーザの ID やパスワードは別途管理されている認証サーバ，グループに含まれるメンバの管理はグループ管理システムで管理する．IP アドレス管理機能では，ID とパスワードを認証サーバ，ID とグループ名をグループ管理サーバに送ることで認証認可を行う．

IP アドレス管理機能側では，グループ管理システム上のグループ名（和名）をネットワーク名，グループ ID をネットワーク ID（英名）として扱う．

機器管理者が MAC-IP 監視管理システムにログインする際，専用の Web サイトにアクセスし，ID とパスワードを入力し，該当のネットワーク名を選択し，ログインボタンをクリックする．その際に，グループ管理システムに ID とネットワーク名を送る．機器管理者がネットワーク名を選択しやすいように，ログイン時のネットワーク名は和名表記とするが，グループ管理システムに送る際には，ネットワーク ID すなわちグループ ID に変換した情報を送る．入力された ID が選択されたグループ ID に含まれるか否か照合し，

含まれる場合は，認証サーバにて ID とパスワードの照合を行う（図 5-5）.

機器管理者が IP アドレス管理機能にログインすると，それぞれに割当てられた IP アドレスの範囲が表示され，指定範囲内において接続機器の登録を行う．登録された機器は，データベース上の MAC-IP テーブルに登録され，ネットワーク監視機能により接続可能になる.

自身が管理者となっている別のネットワーク範囲を管理する場合は，一度ログアウトし，再度ログイン時にログインしたいネットワーク名を選択する.

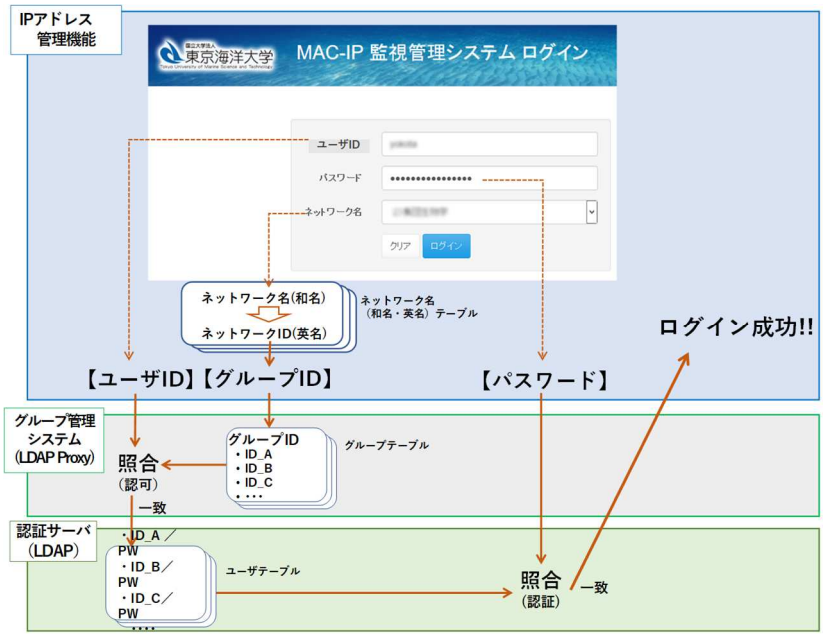

図 5 - 5　IP アドレス管理機能の認証認可の流れ

これまでのグループ管理システムと連携サービスでは，各サービスの管理者がグループを作成しメンバ管理を行っていた．また，一つのサービスに対するアクセス先は，1 ユーザにつき 1 つと想定され運用されてきた．そのためユーザはグループを意識することなく ID とパスワードだけでログインしていた.

しかし，ネットワーク管理システムでは，機器管理者をグループとすることより，システム管理者が複数のグループ管理を行うことは非常に難しいことや，1 人が複数の研究室の機器管理者となる場合があるまた，1 人が複数のグループの管理者になる場合も想定される．そこで，ネットワーク管理システムでは，ユーザのログイン時に ID とパスワードだけでなくログインするネットワーク名（グループ名）を選択することとする.

ネットワーク名を選択する際，初回のみ登録されている全ネットワーク名がプルダウン

形式で表示されるが，一度選択することで，ブラウザに記憶させることにより，次回以降は前回選択したネットワーク名が表示される．

ネットワーク管理機能は全学的な資産管理業務の一部して使用するシステムであることより，グループは，グループ管理者の退職時などにグループが削除されないよう公式グループとして登録する．公式グループでは，グループ管理システムのシステム管理者が，グループを作成し，それぞれの研究室ごとの管理責任者をグループ管理者として登録する．グループを作成する際のグループ名（和名）は，グループ管理システムのログイン時に選択するネットワーク名になることより，所属の研究室名など分かりやすいものとする．グループが作成されれば，グループ管理者が，資産管理の業務を移譲したい人をメンバに追加し，以後追加変更などの管理を行う．

本研究で作成するグループは，研究室などの中でも資産を管理する人だけで構成することより比較的少人数であるため，多くが属性型ではなく，列挙型により作成されることになる．

5.3.4 接続機器などの管理のための操作

機器情報を登録する際，該当グループに割り当てられている IP アドレスの一覧が表示されることより，IP アドレスに対して，MAC アドレスや機器の種類，機器の利用者，利用場所などの必要情報を登録する．接続機器の変更したい場合は，該当機器が登録されている箇所の情報を更新する．機器情報の削除時は，削除が必要な行にチェックし，削除ボタンをクリックする（図 5-6）．

なお，機器名は IP アドレス割り当て時に，ネットワーク名を使って自動割り当てするため，機器管理者は設定しない．システム管理者は，研究室（グループ）ごとに IP アドレスの割り当てを，あらかじめ行う．

図 5 - 6　機器情報の管理画面のイメージ

5.3.5 ネットワーク接続時の動き

MAC アドレスが登録されている機器を，ネットワークに接続すると，DHCP サーバにより，IP-MAC テーブルに登録された IP アドレスを払出す（図 5-7）.

IP アドレスの払出すために，以下の機能を兼ね備えている.

- DHCP サーバ
- DHCP サーバ設定機能
- DHCP サーバログ設定・保存機能

MAC アドレスが未登録の場合，IP アドレスを払い出さないようにするために，以下の機能を備えている.

- パケット抽出機能
- 未登録機器検出機能
- パケット抽出・未登録機器検出のログ保存

この機能により，IP-MAC テーブルに登録されていない機器は，学内ネットワークに接続しても，ネットワークにはつながらない．なお，IP-MAC 登録機能としては，IP-MAC 管理テーブルに以下の情報を格納している.

✧　ネットワーク名

✧ ホスト名

✧ IP アドレス

✧ MAC アドレス

本システムでは，全てのキャプチャできるパケットを解析して DB 化している．これを基にして，その DB 化しているパケットのうち IP-MAC テーブルに関する情報を抽出している．この DB 化，別のパケットの抽出が必要な場合に，容易に対応が可能となる．

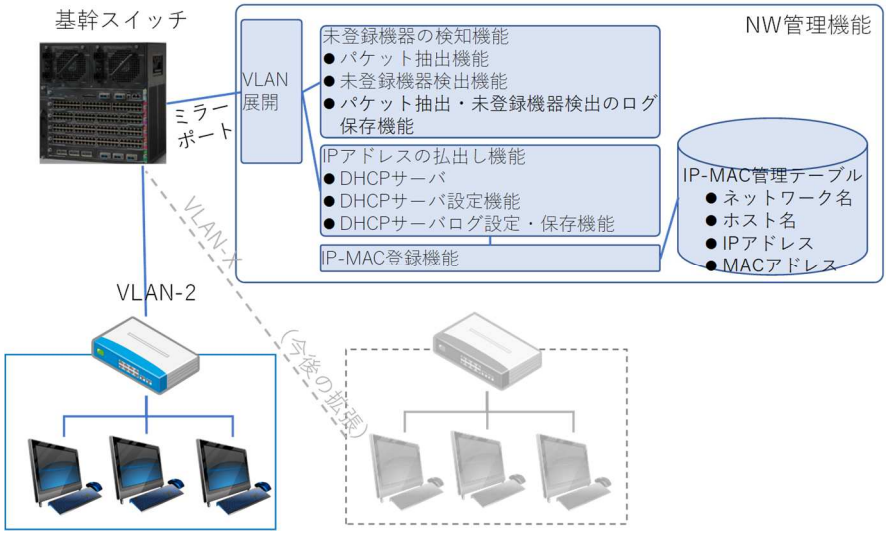

図 5 - 7　接続機器のネットワーク接続時の動き

5.4 MAC-IP 監視管理システムの試験運用

本研究で提案する MAC-IP 監視管理システムを，東京海洋大学品川キャンパスにおいて，2014 年 3 月より 1 研究棟に試験導入し，2015 年 3 月より全研究棟に導入し，2016 年 3 月まで試験運用を行った．

5.4.1 第 1 回試験運用

1 回目の導入においては，2014 年 3 月から試行的に，東京海洋大学品川キャンパスで改修工事のため一時ネットワーク停止していた建物（2 号館）を対象に， MAC-IP 監視管理システムを導入した．該当の建物内には 13 研究室が存在しており，2014 年 7 月時点で 252 件の MAC アドレスが登録されている．導入当初に該当教職員全員に一斉メール

で新システム移行を通知し，機器管理責任者向けの操作マニュアルと利用者向けの詳細な設定マニュアルを添付するとともに，学内 Web サイトで公開した．当初，MAC アドレスの調査ミス・入力ミスなどにより機器管理責任者から問い合わせが数件あったが，その後は，問い合わせはほとんどなく順調に稼働している．MAC-IP 監視管理システムの運用および機器のネットワーク接続方法は 3 か月で概ね浸透したと考えられる．MAC アドレス認証未登録機器（未許可 PC・プリンタ）および規定外接続機器（固定 IP アドレス設定）の接続件数は，当初は 1 日あたり 20 件程度検出される日もあったが，システムの利用方法の周知により平日でも 10 件未満に減少した（図 5-8）．すなわち，2013 年 11 月の調査では未登録・不一致機器件数が 72%あったのに対し（図 5-1），システム導入後の未登録機器は登録件数の 4%未満に抑制できたことから，キャンパスネットワークの安全性は格段に向上したと考えられる．

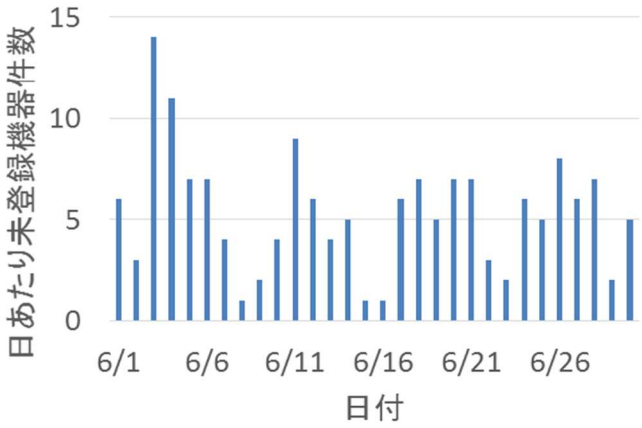

図 5 - 8　未登録機器検出のログ集計結果（2013 年 6 月）

利用者にとっては，これまで紙ベースの申請により，ネットワークに接続でいるのが申請から 2-3 日かかることもあったが，機器管理者が本システムにログインし，機器情報を登録すれば即時にネットワーク接続ができるようになるというメリットもあった．また，DHCP 機能を使うことにより，個々の利用者の機器に IP アドレス等の設定をする負担が軽減され，利用者の利便性向上につながったと言える．機器に IP アドレス等の設定が不要になったことにより，これまで設定ミスにより，約 1 か月に 1 度程度の割合で発生していた IP アドレスの競合件数が，本システムを導入してから約 5 か月の間 0 件であった．

本システムの課題としては，MAC アドレスが登録されている機器に，IP アドレスを設定した場合，その IP アドレスが，異なっていた場合でも，ネットワークに接続すること

ができる．そのため，IP アドレスの競合が発生する可能性もある．現時点では，機器に IP アドレスを登録しないよう運用でカバーしているため，IP アドレスの競合は発生していない．発生した場合でも，これまでに比べると正しい MAC アドレス情報が管理されているため，該当機器の調査の時間が大幅に削減されることが期待された．

5.4.2 第 2 回試験運用（拡張）

1 回目の導入時の運用状況から，本システムを他の 8 研究棟を含む全研究棟へ拡張可能と判断され，全研究棟に試験的に導入することになった．導入は全学的なスケジュールと調整し，2015 年 3 月と設定してスケジュールを作成した．1 回目の 2014 年に導入した 1 研究棟は建物の改修工事完了直後に，建物内全てのネットワーク機器を本システム導入とほぼ同時に設置したため，利用者のシステム変更への意識が高く，後述するネットワーク機器の設定上のトラブルは少なかった．しかし，8 研究棟への導入時には，建物改修などは行われないため，建物ごとに問合せ対応として 4 名の教員を配置し，システム管理部局には専用窓口を設置して非常勤職員を配置し，利用案内やトラブル対応に努めた．また，利用者に対して，本システムを導入するネットワーク（研究棟のネットワーク）とそれ以外の研究棟ではない本部事務棟，講義棟および実験棟などのネットワークと区別がつくよう，全研究棟に導入したネットワークを通称「品川キャンパスネットワーク 2015（S-NW2015）」とした．

S-NW2015 の導入は 2015 年 3 月 23 日に行い，対象は 2014 年度の 1 研究棟 14 研究室から 9 研究棟 97 研究室となり，機器数については約 300 台から 3500 台以上が管理・監視対象となった．

[1] 接続機器の分類

本システムでは，機器情報である MAC アドレスが登録されており，IP アドレスが自動取得設定されている機器が正しい接続方法である．本稿では便宜上，これを機器 Type A とする．ただし，機器により IP アドレスが自動取得設定できない機器も存在する．そのような機器については，例外的に IP アドレスを固定で設定する．これを機器 Type B とする．IP アドレスを固定で設定する際には，正しい IP アドレスを設定する機器と入力ミスなどにより誤った IP アドレス（不正な IP アドレス）が設定される機器が存在する．これを機器 Type C とする．

また，MAC アドレスが未登録で，IP アドレス自動取得設定にして接続している機器

（機器 Type D），MAC アドレスが登録されていないため，IP アドレスが割り振られているはずがないにも関わらず，不正に IP アドレスを設定している機器（機器 Type E）が存在する（表 5-2）．これらを機器 TypeA～E のうち，不正に接続している可能性が考えられる機器 TypeC，D，E について次項以降で，詳細な調査結果を述べる．

表 5 - 2　接続機器の分類

	IP アドレス自動取得（DHCP 自動割当て）設定機器	IP アドレス固定設定機器
MAC アドレス登録済機器	◎　（機器 Type A）	正しい IP アドレス設定 ○　（機器 Type B）
		不正な IP アドレス設定 ×　（機器 Type C）
MAC アドレス未登録機器	×　（機器 Type D）	×　（機器 Type E）

（◎ 正しい利用方法で接続されている機器　○DHCP 自動設定不可機器など例外的な利用方法で接続されている機器　　×不正利用の可能性が高い機器）

[2] 不正利用機器の検出

システム拡張後の不正利用機器数について，1 研究棟から引き続き，同様の検出機能のモニタリングから不正利用機器アクセスログを取得する．なお，不正利用機器は表 5-2 の分類では，不正 IP 設定機器は機器 TypeC，E であり，自動 IP 未登録機器は機器 Type D を示している．図 5-9 は，3 月 12 日から 6 月 4 日までの 1 日毎の不正利用機器台数の推移を示す．

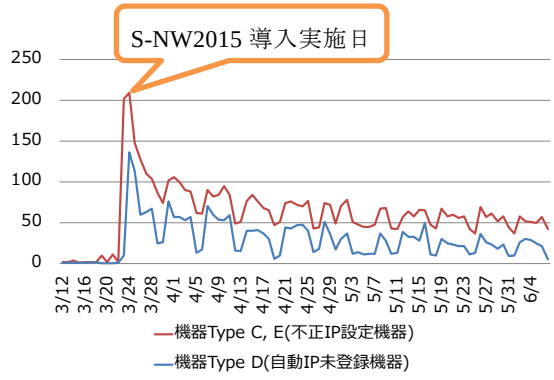

図 5 - 9　日別不正利用機器アクセスログ台数（2015 年 3-6 月）

3 月 22 日以前の導入前の 1 研究棟のモニタリングから 23 日に不正利用機器の接続は一旦急増し，週末と平日の利用者の増減を繰り返して徐々に件数は減少している．6 月 5 日以降も機器 Type D の 1 日当たり件数は平日で 15 台前後，機器 Type C，E も 40 台前後で推移している（8 月 1 日時点）．不正利用機器台数の推移では，2014 年度の 1 研究棟への導入と同様に運用は安定化したように判断される．しかし，S-NW2015 の導入当初は，1 研究棟の時に比べて問合わせが非常に多く，不正利用機器数も非常に多かった．導入 3 か月後でも不正利用機器数は依然として 30～50 台存在し，2014 年 3 月の 1 研究棟での導入の際にはなかった様々なタイプのトラブルが発生した．

[3] 利用者からの問合せ・トラブル

第 2 回試験運用を開始した 3 月 23 日以降の専用窓口および 4 月 15 日以降は，システム管理部局宛に S-NW2015 関連でメールあるいは電話で問い合わせのあった件数は，140 件であった．3 月 23 日～31 日における平日問合せ日数は 7 日間であったが，3 月の問い合わせ件数は 109 件で全体の 78%となり不正利用機器数と同様に導入直後 1 週間程度の利用者の混乱状況が反映されている．

問合せの内容は，3 月にネットワーク接続不可の問合せが 37 件と最も多く，次いで 4 月にも同様の問合せが 12 件であった．また，IP アドレス管理機能に関する問合せも 3 月 10 件，4 月 3 件で，申請方法の問合せは 3 月 10 件，5 月 1 件であった．その他にも，システム変更に伴う大学の Firewall 通過を許可する IP アドレスの再設定や従来までの機器側での IP アドレスの手動入力に関する問合せなど関連する問合せがあった（表 5-3）．

表 5 - 3　第 2 回試験運用開始前後の問い合わせ内容と件数

問合せ内容	件数			
	3月	4月	5月	計
学内ネットワーク接続不可	37	12		49
IP管理機能について	10	3		13
システム概要について	11		2	13
申請方法について （接続機器リストの作り方など）	10		1	11
IPアドレスの領域について	2	1	2	5
FW通過設定（切替後の再設定)について	5			5
固定IPアドレスでの接続について	2			2
その他 （プリンタの設定方法，端末情報の確認方法など）	32	10		42
合計	109	26	5	140

期間：2015/3/1～5/31 ※システム切替は2015/3/23に実施

ネットワーク利用者の設定間違いでネットワークが不通となった件数は，2015 年 6 月までで 63 件であった．そのうち最も多かったのは利用者によるルータ（DHCP 機能）の不正利用で 20 件（32%）であった．ルータの不正利用は建物内の正規の MAC アドレス登録機器にも，対外接続できない不正な IP アドレスを配布されるケースやそれらに付随するループ接続が多発したため，問い合わせ件数を増やす原因となった．また，不正利用ルータの検出には現地調査が必須となり，解決に時間を要する場合があった．他には利用者の機器 MAC アドレスの登録ミスなども多かったが，建物間でそれらの件数は大きく異なった．MAC-IP 監視管理システムに関連する問合せは 6 月でも数件発生しているが，全ての対象研究棟で接続不可などの利用者に不利益なトラブルは解消されており，導入以前の不正なルータ設定なども解決し，利用者からの問合わせほとんどなくなっている．問合せの減少により対応職員の業務は軽減し，紙ベース申請による作業も無くなったため，今後事務手続き削減による運用コストの抑制効果につながると考えられる．しかし，利用者自身あるいは機器管理者は気づかず問合せのない不正利用機器の接続は継続して存在しており，他の利用者への影響を与えるため，詳しく調査を行った．

[4] 研究棟ごとの不正利用機器

システムを拡張した 8 研究棟は研究室数や利用者数に差異があるため，不正利用機器や問い合わせ件数にも偏りが生じている．各建物の研究室数と 3 月からのモニタリングしたのべ不正利用機器の検知数の相関性を分析したところ，概ね研究室数に比例して不正利用機器の検知数は増加した．18 研究室および 9 研究棟がある研究棟において不正アクセス件数が少ない傾向があり，研究室に所属する学生，研究員数等が他の研究棟に比べて少なく，ネットワークを利用する時間が少ないことが調査により明らかとなった．また，2014 年に先行して導入した 1 研究棟も既に初期導入時のトラブルは解消されているため不正利用機器件数は少ない（図 5-10 の白抜き点）．

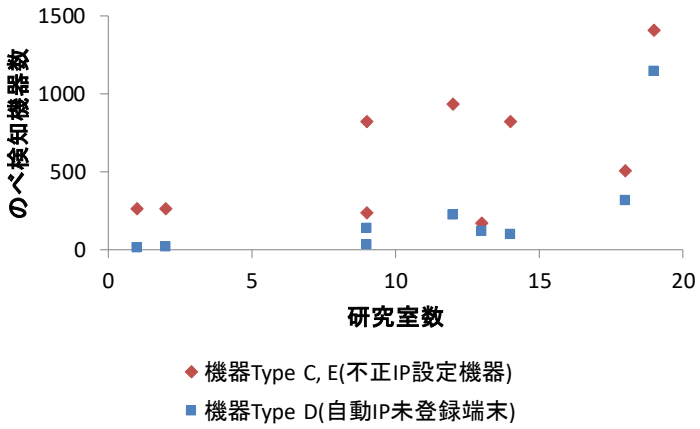

図 5 - 10　各研究棟の研究室通と 3-6 月期の不正利用機器のべ件数の関係

※白抜き点は第 1 回試験運用時に導入の 1 研究棟

5.5 試験運用に対する課題対応と評価

約 3 か月間，S-NW2015 の運用を行った結果，いまだ解決されない不正利用設定機器の対応について検討を行った．スイッチング機器（HUB）やルーティング機器（ブロードバンドルータ）の誤った設定により，非常に問い合わせが多く，場所や該当機器の特定に非常に多くの時間を費やした．しかし，機器管理者に研究室内の HUB やルータの適正な利用方法についての数回の周知の効果により，6 月以降は発生していない．今後の発生可能性を考えると対応方法の改善が必要であるが，現時点では緊急の問題ではないため，今後の課題として本稿では省略する．

5.5.1 不正利用機器の個別調査

不正利用機器の可能性が高い機器には，表 5-2 の通り，以下の 3 パターンが存在した．

- 機器 Type C：MAC アドレス登録済みであるが，IP アドレスが誤って設定されている機器
- 機器 Type D：MAC アドレス未登録であり，IP アドレス自動割当設定されている機器（ただし，正しい IP アドレスが割当てられなかった時に割当てられるリンクローカルアドレス（169.254.xxx.xxx）が設定された機器も含む）
- 機器 Type E：MAC アドレス未登録であり，不正に利用可能な IP アドレスの設定がされている機器

これらの 3 パターンの機器の利用方法に関する個別の調査を行った．調査には，不正利用機器アクセスログを使用する．不正利用機器アクセスログから得た情報から該当建物の建屋スイッチおよびフロアスイッチの MAC アドレステーブルから接続ポートの探索を行う．MAC アドレステーブルから利用履歴が取得できたものについては，接続ポートの判明後，実際に接続ポート先の研究室を訪問し，該当機器の探索を行った．調査期間は，第一回調査期間が 2015/6/8～6/19，第二回調査期間が 2015/7/6～17 のうち平日の 19 日間である．

不正利用機器アクセスログ中からランダムに抽出した 40 件に対して，調査を行った．全研究棟において，それぞれ 1 件以上と抽出されるようにした．抽出された機器 Type の内訳は，

- 機器 Type C　8 件
- 機器 Type D　10 件
- 機器 Type E　22 件

であった．

5.5.2 不正利用機器個別調査の結果

i. 機器 Type C の調査結果

機器 Type C の多くはプリンタなど機器自体に IP アドレスを固定で設定しなければならない機器であった．調査対象機器のうち 7 件が設定していた IP アドレスは，接続ポート先である部屋に割当てられている IP アドレスの範囲内のものであった．うち 1 件は，同研究棟内の別の研究室に割当てられている IP アドレスが設定されていた．利用者に確認を行ったところ，悪意はなく，機器の IP アドレス設定時の入力ミスであった．直ちに該当ユーザに設定を修正してもらった．

ii. 機器 Type D の調査結果

機器 TypeD のうち，特定できた機器は 2 件，特定できなかった機器が 8 件あった．特定できた 2 件の機器は，2 件ともブロードバンドルータであった．ヒアリングを行ったところ，2 件とも HUB だと思っており，機器情報を登録していなかったとのことであった．

直ちに各該当機器の機器管理者に機器の MAC アドレスを登録してもらった.

特定できなかった 8 件は, 該当部屋内には接続機器が多く煩雑になっているなどの理由により，発見できなかった.

機器 TypeD については，本調査時以外にも，問合せが多かった内容である．これまでの問合せがあった際に調査を行った結果, 機器の MAC アドレス登録時に誤った情報が登録されたり, 登録したつもりがうまく登録できていなかったなどの理由により, 正しい IP アドレスが割り当てられない場合がほとんどであった.

MAC アドレスの登録ミスが発生する原因は，該当機器の MAC アドレスを確認する時に，利用用途とは異なる Wireless 用の MAC アドレスなどが登録されていた．これらについては，MAC アドレス確認用のマニュアルをわかりやすく修正を行っている.

iii. 機器 Type E の調査結果

調査の結果，設定されていた IP アドレスは該当の研究室に割当てられている範囲内のものが 13 件あった．そのうち機器が特定できたのは 5 件であった．それぞれ該当の機器管理者と利用者にヒアリングを行ったところ，悪意はなく，機器管理者の MAC アドレス登録ミスが 4 件，利用者の機器の IP アドレスの入力ミスが 1 件であった．直ちに該当者に登録情報もしくは機器の設定を修正してもらった．しかし，8 件は，該当部屋内に非常に多くの接続機器があり，その中には起動していない機器や，接続経路が複雑になっていることもあり，該当部屋内で発見できなかった.

設定されていた IP アドレスが該当の研究室に割当てられていない残りの 9 件についても，該当部屋内には接続機器が多く煩雑になっているなどの理由により，発見できなかった.

iv. 調査結果のまとめ

調査を行った 40 件中 15 件の機器が特定できたが，25 件の該当機器の特定はできなかった（図 5-11）.

特定できなかった機器が設置されている研究室の訪問調査により, 全て学生が主に使用する教室（学生室）であることが判明した．学生室では，該当研究室所属以外の学生や学外訪問者も頻繁に出入りし，持ち込みのノート PC をむやみに LAN ケーブルに接続するなど様々な状況をヒアリングできた. 学生室は接続機器の管理も他の部屋に比べて緩く自由度が高いため，状況は極めて複雑で，発見が困難であった.

これらより，本研究では，機器 Type C は単なる IP の設定ミス，特定できた機器 Type D は，機器の MAC アドレスの設定ミスである場合が多い．これらは，悪意があるとは言い切れないが，特定できなかった機器 Type D と機器 Type E については，MAC アドレスを登録しておらず, かつ, 割り当てられていない IP アドレスを設定していることより，悪質な利用者と考えられる．

この状況を踏まえて，特定できなかった機器 Type D と機器 Type E については，早急に対策する必要があると考え，遮断試験を行い，遮断された機器の動向を調査した．

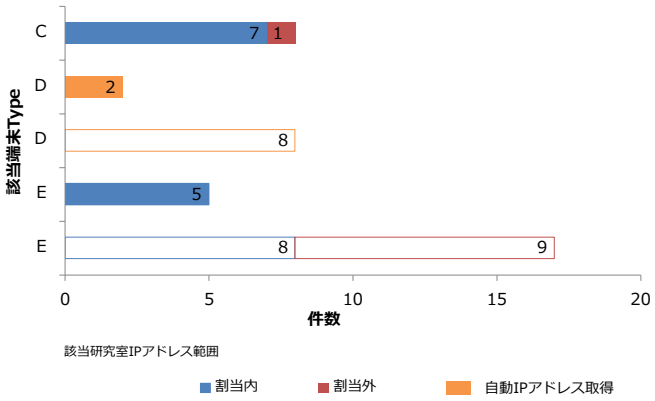

図 5 - 11　不正利用機器の個別調査（40 件）

5.5.3 不正利用機器遮断試験

上記調査期間において，特定できなかった機器 Type D 8 件と機器 Type E 17 件の合計 25 件（図 5-11）に対して，遮断試験を行った．

遮断試験の開始日は 2015 年 7 月 17 日とし，遮断方法は，該当機器の MAC アドレスを該当建屋スイッチに手動にて一時的に遮断する設定を行った．遮断した機器が正しい MAC アドレス情報を登録し直すことを考慮し，1 日に数回，該当機器の MAC アドレスを MAC-IP 監視管理システムでの登録状況を確認した．正しく MAC アドレスが登録されれば，該当の建屋スイッチから遮断設定を解除し，接続可とした．

遮断試験の開始から 1 日以内に，機器情報が登録された機器は 25 件中 3 件，2 日以内に登録された機器は 3 件あった(表 5-4).

表 5 - 4　遮断試験結果のまとめ

試験開始からの日数	件数	遮断設定	
1 日以内	3*	建屋スイッチ	登録確認→解除
1 日～2 日以内	3*		登録確認→解除
7 日～8 日以内	2*	建屋スイッチ	登録確認→解除
継続中	17	(開始 1 週間) →フロアスイッチ (1 週間以降)	2 週間モニタリング接続 記録無

*学生使用の PC

試験開始の 1 週間経過しても依然として機器情報が登録されず, 機器の特定に至らない 19 件について該当の各フロアスイッチにて，該当機器の MAC アドレスに対して遮断設定を行った．フロアスイッチへ遮断設定を開始してから 1 日以内に機器情報が登録された機器は 2 件あった．登録された機器 8 件のそれぞれの機器管理者にヒアリングを行ったところ，全て学生から PC の接続要望があり，該当機器の登録を行ったとのことであった．

さらに特定できない 17 件に対して，フロアスイッチへ遮断設定を行った翌日から該当機器が接続されるか否かのモニタリングを行った．モニタリング期間は約 2 週間としたが，いずれの機器も接続した形跡はなかった．更に，各該当研究室の機器管理者にヒアリングを行ったところ, いずれも本システムの導入を知らない学生あるいは一時訪問者が個別調査と同時期に個人所有 PC の接続を試みたことにより調査記録に残った可能性が高いと判断された．

5.5.4 不正利用機器の傾向と今後の対策

不正利用機器に対する調査を行った結果，悪意の利用者は見当たらなかったが，機器管理者が把握できない部屋で, 学生持ち込み PC など未登録の機器がネットワークに接続されていた．これらの不正利用機器のうち，何度かインターネット接続を試みた後に機器管理者に登録を依頼するケース，ネットワーク接続を取りやめるケース，ネットワーク接続したまま放置するケースなど様々であった．

これらの不正利用機器を検知する度に, 該当機器の接続場所を特定して現地調査を行う

ことや，遮断設定を行うことは，システム管理者の作業負担が大きい．遮断設定を行う場合には，機器情報が登録されれば都度解除設定を行う必要もある．手動で行うことにより，設定ミスや解除の見落としなどの可能性も高まる．

そのため，不正利用機器を検出した時点で，自動的に該当の建屋スイッチもしくはフロアスイッチにて，該当機器の遮断設定を行い，機器情報の登録確認や解除設定が行われることが望まれる．

IP アドレスと MAC アドレス，接続部屋などを登録し，登録情報と異なる場合に検知する仕組みは，これまでにも開発されている[110]．しかし，検知のみでは，システム管理者の手動操作などが必要であり，負担が大きくなる．また，各研究棟のフロアスイッチに認証機能付きのスイッチを導入するには追加の費用がかかり，容易ではない．

そこで MAC-IP 監視管理システムでは，既に不正利用機器アクセスログ機能を保持しているため，それらを用いることで，不正接続機器を検知した際，該当機器を自動的に接続不可にする仕組みの実現が可能となる．

不正利用機器を検知した時点で，その機器が接続されている建屋スイッチ（もしくはフロアスイッチ）に対して，該当機器の MAC アドレスを遮断する設定を行うコマンドを送信する．同時に，遮断機器のリストを作成する．次に，IP アドレス管理機能に機器情報登録後，遮断機器の MAC アドレスが新しく登録されているか否かを照合する．新しく登録された場合は，該当の建屋スイッチに該当機器に対する遮断設定を削除し，遮断機器のリストからも該当機器情報を削除する（図 5-12）．これらの機能を追加すれば不正利用機器の自動遮断が実現可能となる．

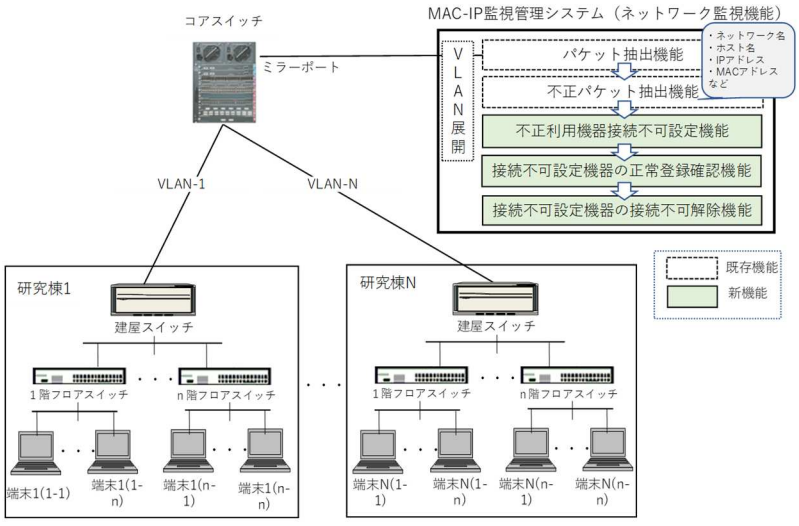

図 5 - 12　不正 IP 設定機器の自動遮断機能追加の概要

5.5.5　IP アドレス管理機能とグループ管理システム連携の評価

IP アドレス管理機能では，教授や准教授，事務局スタッフであれば係長以上の役職の人が機器管理責任者として，システム管理者がグループ管理者に登録する．機器管理責任者として登録された人が，秘書や博士研究員，大学院生，事務局の係員や非常勤職員などを副機器管理者としてメンバに追加登録する．機器管理責任者は他の資産管理システムが導入された際にも担当の責任者となる人であり，副機器管理者は担当責任者から担当業務を移譲される人である．多くの資産管理システムにおいて各研究室の担当者が同じになる場合が多い．

第 2 回試験運用時の 2016 年 3 月時点，IP アドレス管理機能で使用するグループは，約 150 の公式グループが存在した．その中にはグループ管理者が同じでメンバが異なるグループが 3 グループあり，別途，グループ管理者用のグループを管理していた．

作成されたグループの大半が列挙型により作成されたグループであった．また，グループ管理者に与えられた参照権限の範囲を越えたユーザをメンバとしている場合が大半であった．グループごとに管理されている IP アドレスと登録されている機器台数の平均は 20～30 台であるが，少ないところでは 2-3 台，多いところでは，約 80 台の機器が登録され管理されていた．登録機器の変更は，ほぼ毎日数件発生していた．グループ管理者の変更はほぼ無く，メンバの変更は，1 か月に 2-3 件であった．

IP アドレス管理機能の認可として使用するグループ機能は，提案中のグループ管理システムを用いることにより，グループ管理者の参照権限外のユーザでもメンバにできることで，身分や所属が異なる教員や学生などを含めたグループを作成できる．また，ユーザの身分や所属などの属性により，参照権限の条件式を定めておくことにより，グループ管理者を設定する度に参照権限の設定は不要になる．公式グループという概念により，グループ管理者不在にも即時削除されることがなくなる．公式グループでは，グループ管理者用のグループを作成できることにより，複数のグループの管理者が同じ場合，一カ所で管理できることになった．

グループ管理システムでは，これまで連携してきたサービスは，ユーザは所属グループを意識することなく，ID とパスワードを入力するだけでログインできていた．また，各サービスの管理者がグループ管理者となりメンバを管理していた．そのため，ユーザがグループやネットワーク名を意識してログインすることが無かった．本研究においては，ユーザにグループという概念を用いることで混乱をきたす可能性があったることより，でき

る限りユーザがグループを意識しなくてよいよう, ネットワーク名であるグループ名は所属建物と研究室名が分かる名前とした. またネットワーク名という名称も定着していなかったことより, ログイン時の Web インターフェースでは, ネットワーク名の選択時には, 操作したい研究室名を選択すればよい運用とした. また, 本研究で提案する仕組みでは一ユーザである教授や准教授がグループ管理者となり, システム上でメンバを管理するという操作が増えたが, 都度変更申請を行う手続きを行うことなく, 自身の裁量でリアルタイムにメンバ変更できることより, 利便性の向上につながったと言える.

各機器管理者にグループの概念や操作が定着されていることにより, 接続機器情報やメンバ情報の変更の際に, 変更手続きが不要で変更操作がリアルタイムに反映されること, 流動性の高い秘書や大学院生などでもグループ管理者が簡単に登録・削除できることにより, 全体的には利便性が向上したとの意見も多かった.

本研究において作成したグループは, 複数の資産管理システムの認可として応用できることを期待するが, 研究室内でも資産管理システムごとに管理するメンバが異なる場合も考えられる. 現提案中のグループ管理システムでは, グループのメンバが異なる場合は, 新しいグループを作成しなければならない. 特に予算などの管理システムの利用制限はネットワーク管理システムより厳格である可能性が高い. グループ管理者に当たる人のみが利用することも考えられる. メンバには秘書は含むが学生は含まないという場合には, この限りではない. これらにおいては, 今後の課題として実運用と照らし合せつつ検討していく必要があると考えている.

5.5.6 提案の仕組み導入による具体的な効果

本研究で提案する仕組みを導入することにより, ネットワークの管理運用においては, 接続機器の追加や変更の都度発生する登録や削除の操作にかかるコストだけでなく, トラブル時の対応にかかるコストも削減された.

具体的には, 約 3,000 のネットワーク機器の接続に対して, 変更や追加が発生する件数は, 1 か月あたり平均 15 件程度とし, それ以外にも登録されている情報の一覧要請などもが 1 か月あたり平均 2 件程度あったことより, 1 か月にかかる作業を 10 人日, 作業 1 人日を 10,000 円と仮定すると, 1 年間で約 1,200,000 円が削減されたといえる. また, ネットワークトラブルは月平均 2〜3 回発生しており, その度に作業が必要であり, 作業は約 5 人日と想定すると, この削減を数値で表すと, 1 か月あたりのトラブルを 3 回, 作業の 1 人日を 10,000 円として仮定すると, 1 年間で約 1,800,000 円が削減さ

れたことになる．合わせて 1 年あたり約 4,000,000 円の運用コストの削減ができたと言える．

また，機器管理者にとっても個々に管理されていたネットワーク機器の管理が，Web 上で統一的に行えるようになったことより，申請不要でリアルタイムに追加や変更の操作ができるようになり，申請から承認までに要する時間が大幅に削減された．機器管理者の変更時も申請不要で Web 上から変更可能できるようになり，申請から承認にかかる時間が削減された．利用者にとってもネットワーク接続時に複雑な IP アドレスの設定等を行う必要がなくなったため，ネットワーク接続に要する時間が削減された．

5.5.7 試験運用に関するまとめ

試験運用を行った東京海洋大学品川キャンパスでは，キャンパスネットワークに機器を接続する際，機器情報やユーザ情報などによる制限は無く，研究室内のネットワーク接続機器の管理は紙ベースの申請書と承認書によるものであったため，ネットワーク接続に関する機器の管理が杜撰であった．そのため，IP アドレスの競合や所有者あるいは責任者不明の機器接続によるネットワークトラブルが多発し，解決に非常な時間を要し，システム管理部局の担当者に多大な負担があった．

試験導入では，S-NW2015 を全研究棟に導入することにより，機器の管理を厳格に行えるようになり，トラブル発生時も比較的迅速に対応可能となった．

また，ユーザのネットワーク利用に関する意識も全体的に向上し，ネットワークトラブルの発生頻度が大きく低下した．トラブル件数は減少したものの，詳細な不正利用機器の調査を継続した結果，杜撰な管理の機器が数台存在するということが分かった．正しく管理されていない機器を接続することにより，学内ネットワークのリスクが高まるため，今後は該当機器を接続不可にする必要がある．しかし，都度操作はシステム管理部局に多大な負担がかかるため，自動的に接続不可とする設定および接続不可解除の設定が不可欠である．

5.6 結語

本研究では， キャンパスネットワークへの接続時に，これまで研究室などの単位で個別に管理されていた接続機器情報の管理方法を統一し，MAC アドレスと IP アドレスのテーブルを照合することにより接続機器の制限を行う MAC-IP 監視管理システムを実装した．また，実装した仕組みを試験運用として東京海洋大学品川キャンパスの全研究棟へ

導入し，その経緯，運用評価，課題について述べた．

提案のシステムを試験導入した当初は，多少の混乱を招いたが，運用でカバーすることにより，安定稼働を行えた．本研究で提案する仕組みを導入することで，接続機器の管理を厳格に行えるようになり，トラブルの削減やトラブル発生時にも比較的迅速に対応可能となり，相対的に運用コスト削減につながる．また，IP アドレス管理機能へアクセスする際にはグループ管理システムと連携したことにより，ユーザにグループの概念が定着されつつあり，今後，他の資産管理するシステムなどと連携する際にもスムーズに受け入れられるようになることが期待される．

本システムにおいては，研究室内において接続機器が正しく管理されることを目的としたが，MAC アドレスは比較的簡単にソフトウェアから変更することができることと，通信が暗号化されないため，高セキュリティレベルでの利用には向かない[110]．今後，悪意のある攻撃者からの対応などセキュリティ強化が求められるようになれば，デジタル証明書による機器認証や利用者認証を組み合せるなど検討が必要になることも考えられる．

第6章　結論

本研究では, 様々な利用者や情報システムなどの管理が分散して行われている大学などの分散管理組織において, 利用者と情報システムを情報サービスとして提供する際のアクセスマネジメントについて, 提供するサービスが組織を越えて利用できる統一的な仕組みになることを目指しつつ，その前段階として，個別課題を取り上げ，組織内向けの仕組みとして検討を行った．具体的には利用者，情報システム，それを情報サービスとして提供する際のアクセスマネジメントにおいて，それぞれ一時利用者向け IC カード認証，統合 ID と属性を用いたグループ管理，キャンパスネットワークと接続機器の管理の 3 つの個別課題を取り上げ，それぞれの課題において，分散的に管理される実態に合わせて，各管理者がそれぞれ分散的に効率的に管理できる仕組みとし, 安全性を確保しつつ管理運用に関するコストを低減する仕組みの検討を行った．また，それぞれの個別課題においては，システムの実装し，試験稼働と評価を行った．

本研究において提案した仕組みは，それぞれの管理者に対する観点より，安全性を考慮しつつ分散的に管理されている実情と合わせて分散的に管理できるようにすることで, 従来の仕組みと比較すると各管理者の負担の軽減を行うことになり, 全体の管理運用コストの低減に繋がった．

一時利用者向け IC カード認証では，IC カード認証の仕組みを導入する際に組織内で一元的に把握が困難な一時利用者に対して，都度 IC カードを発行することなく，本人が日常的に利用している IC カードを用いて認証サービスを利用するための仕組みについて検討した．認証にはサービスのレベルに応じてセキュリティレベル分けを行い，それぞれのレベルに合わせた認証方式について検討を行った. セキュリティレベルが比較的低いサービスにおいては一般カードのカード内の読み取り可能な情報だけを用いる. セキュリティレベルが中のサービスにおいては，カード内情報と PIN コード，さらにセキュリティレベルが中上のサービスにおいては，カード内情報と PIN コードに ID とパスワードを組み合わせる仕組みとした. PIN コードを用いた認証を行う際には, 一般カード内に新たに PIN コードの情報を格納することが難しいため, 一般的にはシステム側に格納するが, 本研究では, システム側に情報を格納することによるシステムの管理者の管理の負担を軽減するため，本研究ではシステム側にも一般カード側にも情報を格納せずに，一般カードの読み取り可能な情報から PIN コードを生成する PIN コード生成方式を提案した．提案の仕組みは，部局などの単位で導入でき，その際に部局などのシステム管理者は，システム側で PIN コード生成用のプログラムと PIN コード認証用のプログラムなどを格納する

だけで，一時利用者の IC カードや PIN コードの管理が不要となる．これにより，各サービスの管理者は IC カード認証を行う際，一時利用者に対して IC カードの発行することなく，かつ，PIN コードの管理も不要とすることより，相対的な管理運用コストの削減を実現した．

統合 ID と属性を用いたグループ管理に関しては，依然として普及が進まない部局などが管理するサービスに対する認可の統合化において，各サービスの認可情報の管理に，グループ機能を用いることで．各サービスが分散的に管理される実態と合わせて，システム管理者とグループ管理者が効率よく管理できる仕組みの検討を行った．

検討の仕組みでは，これまでのグループ管理の仕組みで課題となっていたグループに対する柔軟性と継続性に対して，一般ユーザが参照権限にとらわれずに自由に作成可能な「一般グループ」と，グループの重要度に合わせて継続性を確保する「公式グループ」の二種類のグループに分け，これらの 2 つのグループを使い分け，グループの管理を分散的に行うことで，システム管理者からグループ管理者，そしてグループ管理者から新グループ管理者へ，円滑にグループ管理の権限移譲を行えるようになり，相対的な管理コストの削減を実現した．キャンパスネットワークと機器の管理に関しては，これまで研究室などの単位で個別に管理されていたネットワーク接続機器の管理について，組織内において統一化し，これまで研究室などの単位で分散的に管理を行っていた実態と合わせて，分散的に管理するための仕組みの検討を行った．検討の仕組みでは，4 章で提案したグループ管理システムと連携することで，研究室などの単位における機器管理者をグループとして管理することで，機器管理者の追加や変更をグループ内でスムーズに行うことができる仕組みとした．また，利用者の安全性を確保するため，ネットワークに接続時に，登録されたネットワーク接続機器情報を用いて，MAC アドレスと IP アドレスを関連付けして認証することで，機器の監視，通報，遮断する仕組みを取り入れ，「MAC-IP 監視管理システム」として実装を行った．これにより，迅速な登録情報の変更や，トラブル発生時の迅速な調査に対応可能になるなど，相対的な管理運用コストの削減を実現した．

これらより，本研究で取り上げた個別課題は，安全性を確保しつつ，分散的に管理されている実態と合わせて分散的に効率的に管理できる仕組みであり，各管理者の管理の負担を軽減することが実現でき，管理運用に対するコストの低減につながった．

本研究で提案した仕組みは，大学などの分散管理組織において一つの組織内サービスとして実装したものであるが，本研究で提案した仕組みや概念は，組織を越えたサービスとして応用することが可能である．本研究で取り上げた個別課題は，他の分散管理組織においては同様の課題を有していることより，組織間連携に向けた統一化が期待される仕組み

である.

分散管理組織における利用者や情報システム, そしてそれらに対する情報サービスの管理が, 中央で一元管理されておらず, 分散して行われているという特徴は, 大学などの教育研究組織に限定されるものではなく, グループ会社や子会社等を有する大企業などにおいても同様の課題を抱えている組織が多い. 今後ますます情報サービスが増加することが想定される中, 本研究で提案する仕組みや概念を取り入れ, 組織間を越えたサービスとして統一化し, 提供していけることで, さらに各管理者の負担が軽減され, 管理運用のコストの低減が期待できる.

例えば, 3 章で取り上げた一時利用者向けの扱いに対する提案仕組みにおいては, 本研究で提案する概念を用いることで, 大学の一時利用者に対してだけではなく, IC カードが導入されていない組織の教職員や学生などが利用することも可能である. また, 共通の IC カードが発行することが難しい, 組織を越えたサークルや学会などの組織においても, 専用サイトへのアクセス時に IC カード認証を用いる際には利用することが可能となる. 4 章で取り上げた統合 ID と属性を用いてグループとして管理する仕組みは, 本研究で提案する概念を用いることで, 組織内のグループだけでなく, 組織を越えたサークルや学会などのグループを作ることも可能になる. 作成したグループを用いて, メーリングリストや Web によるスケジュール管理, Web 掲示板の閲覧などが可能になり, 組織を越えたグループの交流にも用いることが可能となる. また, 提案するグループ管理の仕組みの概念は, 利用者に対してだけではなく, 情報サービスをグループとして管理する際にも応用可能である. 5 章で取り上げたキャンパスネットワークと接続機器の管理においては, 組織ごとに IP アドレスやポリシーを設定できる仕組みを追加し統一的な仕組みとすることにより, 複数の組織においてキャンパスネットワークの管理が可能になる. また, 情報システムに対するアクセスマネジメントとしては, 4 章で実装したグループ管理システムと連携することで, 他の薬品や図書などを管理するシステムにも, 応用可能である. 本研究で提案した仕組みの概念を複合すると, キャンパスネットワークと接続機器の管理をする際, 組織外からの認証に IC カード認証を用いたい場合, 一時利用者向け IC カード認証システムの概念を取り入れることで, 機器管理者が保有する IC カードを用いて認証を行うことも可能となる.

本研究で実装した仕組みについて, 組織間連携のサービスとして提供していくためには, Shibboleth による連携が必要となる. 大学間連携においては国立情報学研究所により開発されている GakuNin と連携することが必要となる. 今後, 情報サービスは益々増加していくことより, 各管理者の管理運用の負担を軽減できるよう, 組織を越えた統一的な仕

組みとして提供していくことが求められる．本研究で提案する仕組みを，具体的に組織間連携による統一化した仕組みとする場合には，本研究で提案する仕組みは，利用者の属性情報を必要とすることより，他組織に所属者の属性情報の取り扱いなど安全性に関する更なる検討が必要になる．また，利用者の増加によるアクセス集中による対応も必要になると考える．　本研究において実装した仕組みを統一化することにより，各管理者の管理運用に関する負担軽減だけでなく，各利用者においても各サービスの利用時の負担が軽減される．多くの情報サービスが統一化され組織を越えても利用できるようになることで，利用者にとっては，異なる組織へ行った時や，組織間の異動があった際にも新しく異なる操作方法を覚えなくとも，同様の操作で対応が可能となり，利用者に対する利便性の向上が期待される．

謝辞

本研究を行い本論文の執筆するに至り，非常に多くの方に多大なるご支援ご指導をいただきました．心より御礼申し上げます．

本研究を進め，本論文を執筆するにあたりまして，指導教員の岡部寿男教授には多大なるご指導ご助言を賜りました．心より感謝申し上げます．また，論文審査委員（副査）として貴重なご助言を賜りました森信介教授ならびに緒方広明教授に深く御礼申し上げます．

本論文の各研究テーマを進めるにあたりまして，宮崎修一准教授，国立情報学研究所の中村素典教授，同所属の高倉弘喜教授，株式会社シー・オー・コンブ代表取締役の丸山伸氏，徳島大学の大平健司講師，そして研究室の皆様には多大なるご助言を賜りました．深くお礼申し上げます．

本研究を始めるにあたりましては，相談に乗っていただき岡部研究室を紹介してくださいました情報環境機構の永井靖浩教授，職場で働きながら学位取得を目指せる環境を作ってくだり全面的にご協力くださいました東京海洋大学旧情報処理センター元センター長の吉田次郎名誉教授，そしてその環境を継続してくださり，同じく全面的に協力してくださいました同旧情報処理センター品川地区の副センター長や主任をご担当されました戸田勝善教授，萩原智明教授，横田賢史准教授，鈴木直樹准教授に深謝いたします．

本論文の各研究テーマにおける開発および試験運用におきましては，東京海洋大学旧情報処理センター品川地区のスタッフの皆様に多大なるご協力をいただきました．開発におきましては，株式会社アイティフラッグスの小岩徳明氏，株式会社コネクトドットの星野寛氏に多大なるご協力をいただきました．心よりお礼申し上げます．

最後に，学位取得に向けて常に応援し支えてくれた家族に心より感謝します．

参考文献

[1] 篠崎彰彦「情報技術革新の経済効果 ： 日米経済の明暗と逆転」日本評論社，情報技術革新の経済効果，2003.

[2] 古明地正俊「ユビキタス技術の動向とセキュリティ」第８回コンピュータ犯罪に関する白浜シンポジウム REPORT，pp.6-13，2004.

[3] 独立行政法人情報処理推進機構セキュリティセンター「アイデンティティ管理技術解説」2013.

[4] 古明地正俊「ユビキタス技術の動向とセキュリティ」第８回コンピュータ犯罪に関する白浜シンポジウムＲＥＰＯＲＴ，pp.6-13，2004.

[5] Northwestern University「Identity and Access Management At Northwestern University」Working Group Report，2014.

[6] 内藤久資，梶田将司，小尻智子，平野靖，間瀬健二「大学における統一認証基盤としての CAS とその拡張」情報処理学会論文誌，Vol.47，No.4，pp.1127-1135，2006.

[7] 小松文子「プライバシ保護のためのアーキテクチャ」情報処理，Vol.48，No.7，pp.737-743，2007.

[8] 松平拓也，中村素典，山地一禎，西村健，高田良宏，笠原禎也．学術組織間デジタル資料分散共有システム「ARCADE」の開発．情報処理学会論文誌，Vol.55 No.5，pp.1485-1497，2014.

[9] 飯田勝吉，新里卓史，伊東利哉，渡辺治「キャンパス共通認証認可システムの構築と運用」電子情報通信学会論文誌 B,Vol.J92-B No.10 pp.1554-1565,2009.

[10] 文部科学省「情報教育の実践と学校の情報化～新「情報教育に関する手引」～」2002.

[11] 清水康敬，山本朋弘，堀田龍也，小泉カー，吉井亜沙「学校教育の情報化に関する現状と今後の展開に関する調査結果」日本教育工学会論文誌 ，Vol.30 (4)，pp.365−374，2007.

[12] 江藤博文，渡辺健次，只木進一，渡辺義明「全学的な共通情報アクセス環境のための統合認証システム」情報処理学会研究報告インターネットと運用技術（IOT），Vol.2002，No.95(2002-DSM-027)，pp.31-36，2002.

[13] 松平 拓也，笠原 禎也，高田 良宏，東 昭孝，二木 恵，森 祥寛「大学における Shibboleth を利用した統合認証基盤の構築」情報処理学会論文誌 52(2)，703-713，2011.

[14] 姫野聡也，上田浩，喜多一，森幹彦「学認連携 Moodle における受講者動向分析に向けた小テスト成績と設問に関する一考察」研究報告教育学習支援情報システム（CLE），Vol.2015-CLE-17，No.35，pp.1-6，2015.

[15] 根本淳子，高橋暁子，竹岡篤永「大学連携における e ラーニング教材質保証システムの構築を目指したアジャイル指向アプローチの提案」コンピュータ＆エデュケーション，Vol.42，pp.19-24，2017.

[16] 米満潔，古賀崇朗，永溪晃二，高崎光浩，穂屋下茂「大学コンソーシアムでの同期型遠隔授業の環境構築と実践」教育システム情報学会誌，Vol.29，No.3，pp.165-169，2012.

[17] 阿部一晴，渡邉康晴，桑原千幸，辻健司「大学コンソーシアム京都単位互換制度における e-learning の取り組み」2012 PC Conference，pp.325-328，2012.

[18] 谷口邦彦，中川功一，小林敏男「大学における産学連携の制度整備と共同研究創成活動との関連分析」Journal of International Association of P2M，Vol.10，No.2，pp.165-178, 2016.

[19] MRI 株式会社三菱総合研究所「本格的な産学連携活動の促進に向けた基礎調査」報告書，2017.

[20] Hiroyuki Sato，Takeshi Nishimura「Federated Authentication in a Hierarchy of IdPs by using Shibboleth」Proc. 11th Int'l Symp. Applications and the Internet (SAINT), MIDARCH 2011，pp. 327-332，2011.

[21] 谷本茂明，島岡政基，片岡俊幸，西村健，山地一禎，中村素典，曽根原登，岡部寿男「大学間認証連携のためのキャンパス PKI 共通仕様」，電子情報通信学会論文誌，Vol.J94-B，no.10，pp.1383-1388，2011.

[22] 只木進一，江藤博文，大谷誠，渡辺健次「認証基盤の効率化と「学認」への対応」電子情報通信学会技術研究報告，ICM，情報通信マネジメント，112(22)，45-50，2012.

[23] 島岡政基，西村健，古村隆明，中村素典，佐藤周行，岡部寿男，曽根原登「学術機関のためのサーバ証明書発行フレームワーク」電子情報通信学会論文誌，Vol.J54-B，No. 7，pp.871-882，2012.

[24] 谷本茂明，島岡政基，片岡俊幸，西村健，山地一禎，中村素典，曽根原登，岡部寿男「大学間認証連携のためのキャンパス PKI 共通仕様」，電子情報通信学会論文誌，Vol.J94-B，No.10，pp.1383-1388，2011.

[25] 国立情報学研究所“学認（GakuNin）” https://www.gakunin.jp/ last visited September 8, 2018.

[26] Ineternet2 ”Grouper” http://www.internet2.edu/products-services/trust-identity-middleware/grouper/ last visited September 1, 2018.

[27] “Grouper Wiki Home” https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home last visited September 1, 2018.

[28] 木幡康博，森田康之，及川和彦，山足光義，小宮崇，小杉優「大規模情報系システムにおける統合 ID 管理ソリューションの適用」三菱電機技報 2012 年 7 月号，論文 08，pp．29（399）,2012.

[29] 田中伸佳，桑田雅彦「内部統制時代の統合 ID 管理」NEC 技報，Vol.60，No.1，2007.

[30] 江原康生「大阪大学における新全学 IT 認証基盤システムの構築と運用」電子情報通信学会論文誌 D，Vol.J95-D，No.5，1172-1182，2012.

[31] 渡辺義明，渡辺健次，江藤博文，只木進一，「利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発」情報処理学会論文誌，Vol.42， No.12，pp.2802-2809，2001.

[32] 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明.「シングルサインオンに対応したネットワーク利用者認証システムの開発」情報処理学会論文誌 vol.50,No.3,1-9,2010.

[33] 梶田将司，内藤久資，小尻智子，平野靖，間瀬健二「CAS によるセキュアな全学認証基盤の構築」情報処理学会研究報告インターネットと運用技術（IOT），Vol.2005，No.39(2005-DSM-037)，pp.35-40，2005.

[34] 藤村喬寿，西村浩二，近堂徹，大東俊博，田島浩一，相原玲二「スイッチベースの認証ネットワークへのシングルサインオン機能の実装と評価」情報処理学会論文誌，Vol.53，No.3，pp.958-968，2012.

[35] 文部科学省「学校基本調査における本務者・兼務者の取扱いについて（資料 1-3）」2014.

[36] 永吉実武「業務管理システム構築プロジェクトの成功とプロジェクト環境の関係性に関する一考察」電子情報通信学会技術研究報告.SWIM, ソフトウェアインタプライズモデリング 108(316) , pp.1-6, 2008.

[37] 首相官邸 IT 戦略本部「IT 新改革戦略 -いつでも、どこでも、誰でも IT の恩恵を実感できる社会の実現」2006.

[38] 奥山隆文, 高橋則行, 安川健太, 重成幸生, 宮田高道, 飯田勝吉「ユーザ単位での MAC アドレス認証による運用コスト低減を目的としたセキュアキャンパス公衆 LAN の構築(映像通信, コンテンツ配信ネットワーク, マルチキャスト, 一般)」電子情報通信学会技術研究報告, ネットワークシステム, 105(127), pp.29-32, 2005.

[39] 川橋裕, 坂田渉「組織内ネットワークにおける機器監視システム MARS の構築と運用」学術情報処理研究 No.18, 2014.

[40] 久長穣, 杉井学, 為末隆弘, 金山知余, 小河原加久治「山口大学におけるネットワーク運用支援システム」学術情報処理研究, No.15, 2011.

[41] 平野亮, 森井昌克「パスワード運用管理に関する考察および提案とその開発」, 電子情報通信学会技術研究報告, 信学技報 111(286), pp.129-134, 2011.

[42] 辻尾 寿彦, 松西 英恭「情報システムの認証技術について」電気設備学会誌, Vol.30, No.10,pp.827-830, 2010.

[43] FFIEC「Authentication in an Internet Banking Environment」, 2005.

[44] 山田慈朗, 八木哲志, 上野磯生, 北川毅「多要素認証プラットフォームにおける認証技術組み合わせの評価方法について」情報処理学会研究報告,CSEC-51, No.11, 2010.

[45] 野口宏, 大瀧保広, 高橋幸雄, 鎌田賢「Office365 と Shibboleth の多要素認証対応 SSO 環境の構築」学術情報処理研究, Vol.20, pp.82-89, 2016.

[46] 清水さや子, 横田賢史, 戸田勝善, 吉田次郎「東京海洋大学における全学 IC カード導入と多機能化に向けた取り組み」学術情報処理研究 No. 14, 149-152, 2010.

[47] X. Zhang, et al. PBDM: a flexible delegation model in RBAC, SACMAT'03, pp.149-157, ACM, 2003.

[48] X. Jin, et al. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC, Data and Applications Security and Privacy XXVI, LNCS7371, pp.41-55, Springer, 2012.

[49] Vincent C.Hu, D.Richard Kuhn, David F.Ferraiolo, Jeffrey Voas「Attribute-based access control」IEEE, Vol.48, pp.85-88, 2015.

[50] Toshiyuki Kataoka，Ken Nishimura，Masaki Shimaoka，Kazutsuna Yamaji，Motonori Nakamura，Noboru Sonehara，Yasuo Okabe「Leveraging PKI in SAML2.0 Federation for Enhanced Discovery Service」Proceedings of the 2009 International Symposium on Applications and the Internet (SAINT2009)，pp.239-242，2009.

[51] Wataru Oogami，Takaaki Komura，Yasuo Okabe「Secure ID Transformation for Robust Pseudonymity against Backflow of Personal Information in SAML Federation」Proc. 2012 IEEE 36th International Conference on Computer Software and Applications Workshops (6th IEEE International Workshop on Middleware Architecture in the Internet (MidArch 2012))，pp.64-69，2012.

[52] 清水さや子，岡部寿男，吉田次郎「一般カードを使った一時利用者向け認証システムの設計と実装」情報処理学会論文誌，コンシューマ・デバイス&システム Vol.3，No.1，34–45，2013.

[53] 阿部英司，伊東栄典，笠原義晃，中國真教「認証つきサービスにおける組織間連携のための PKI と OpenID の融合」情報処理学会研究報告インターネットと運用技術 (2008-IOT-002)，pp.17-22，2008.

[54] 塚本芳昭「研究大学における産学連携システムに関する研究」研究　技術　計画，Vol.14，No.3，1999.

[55] 塚本芳昭，清水 喬雄「英国の産学連携システムに関する研究」研究　技術　計画，Vol.15，No.3/4，2000.

[56] 島岡政基，片岡俊幸，谷本茂明，西村健，山地一禎，中村素典，曽根原登，岡部寿男「大学間連携のための全国共同認証基盤 UPKI のアーキテクチャ設計」電子情報通信学会論文誌 B，Vol.J94-B，No.10，1246-1260，2011.

[57] Tananun Orawiwattanakul，Kazutsuna Yamaji，Motonori Nakamura，Toshiyuki Kataoka，Noboru Sonehara「User Consent Acquisition System for Japanese Shibboleth-based Academic Federation (GakuNin)」International Journal of Grid and Utility Computing (IJGUC)，Vol.2，No.4，pp.284-294，2011.

[58] 西村健，中村素典，山地一禎，佐藤周行，大谷誠，岡部寿男，曽根原登「多様なポリシーを反映可能な認証フェデレーション機構の実現」電子情報通信学会論文誌，Vol.J96-D，No.6，pp.1400-1412，2013.

[59] 中村素典，山地一禎，片岡俊幸，西村健，庄司勇木，古村隆明，岡部寿男「学術認証フェデレーションを活用するサービスの展開」第 27 回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会,2010.

[60] Yasuo Okabe，Takaaki Komura，Hiroyuki Sato，Kazutsuna Yamaji，Motonori Nakamura「An Authentication Federation Proxy Which Conceals Attributes and Authorization Policies Each Other」Second IEEE International Workshop on Middleware for Cyber Security, Cloud Computing and Internetworking (MidCCI2016), in Proc. IEEE 40th Annual Computer Software and Applications Conference (COMPSAC2016)，vol.2，pp.202-207，2016.

[61] Tomohiro Ito，Daisuke Kotani，Yasuo Okabe「A Threshold-based Authentication System Which Provides Attributes Using Secret Sharing」The 3rd IEEE International COMPSAC Workshop on Secure Identity Management in the Cloud Environment (SIMICE), in Proc. IEEE 41th Annual Computer Software and Applications Conference (COMPSAC2017)，vol.2，pp.730-737，2017.

[62] Tomo NIIZUMA，Hideaki GOTO「Centralized Online Sign-up and Client Certificate Issuing System for eduroam」The 38th Annual International Computer, Software & Applications Conference (COMPSAC2014)， The 8th IEEE International Workshop on Middleware Architecture in the Internet (MidArch2014) pp.174-179，2014.

[63] 国立情報学研究所“eduroam jp” https://www.eduroam.jp/ last visited September 1, 2018.

[64] 樋地正浩，布川博士，白鳥則朗「自律的オブジェクトによる協同作業のモデル化」情報処理学会研究報告 グループウェア研究会，93(56) ，pp.9-16，1993.

[65] 伊吹塁「”クラウド型”グループマネジメント～グループ価値最大化に向けた戦略的グループマネジメントのあり方～」FAS Group Newsletter，Vol.30, May, 2011.

[66] Exgen Networks ”LDAP Manager” http://www.exgen.co.jp/lm/ last visited September 1, 2018.

[67] T.Nishimura, M.Nakamura, M.Otani, K.Yamaji, N.Sonehara. Group Management System for Federated Identities with Flow Control of Membership Information by Subjects. Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual，pp.94-99，2012.

[68] 西村健，坂根栄作，合田憲人，山地一禎，中村素典「個人属性と集合属性が共存する認証認可モデル」電子情報通信学会技術研究報告，Vol.114，No.216，IA2014-17，pp.19-24，2014.

[69] Hiroyuki Sato，Yasuo Okabe，Takeshi Nishimura，Kazutsuna Yamaji，Motonori Nakamura「Privacy Enhancing Proxies in Attribute Release: Two Approaches」Proceedings of The 7th IEEE International Workshop on Middleware Architecture in the Internet (MidArch 2013), in Proceedings of The 37th Annual International Computer Software & Applications Conference (COMPSAC 2013)，pp.372-384，2013.

[70] Takeshi Nishimura, Motonori Nakamura, Kazutsuna Yamaji, Hiroyuki Sato, Yasuo Okabe「Privacy Preserving Attribute Aggregation Method without Shared Identifier Binding」IPSJ Journal of Information Processing，Vol.22, no.3，pp.472-479，2014.

[71] Facebook「Facebook」https://www.facebook.com/ last visited September 1, 2018.

[72] Google「Google Group」https://groups.google.com/ last visited September 1, 2018.

[73] Blanche W. O'Bannon，Jeffrey L. Beard，Virginia G. Britt「Using a Facebook Group As an Educational Tool: Effects on Student Achievement」Computers in the Schools，Interdisciplinary Journal of Practice,Theory,and Applied Research，Vol.30，pp.229-247，2013.

[74] Gila Kurtz「Integrating a Facebook Group and a Course Website: The Effect on Participation and Perceptions on Learning」American Journal of Distance Education，Vol.28，pp.253-263，2014.

[75] 上原哲太郎，清水晶一，永井靖浩，古村隆明，喜多一「大学における認証 IC カードの導入状況」情報処理学会研究報告-インターネットと運用技術（2009-IOT-4），pp.253-258，2009.

[76] 安浦 寛人「九州大学全学 IC カード導入プロジェクト」九州大学大学院システム情報科学研究院　21 世紀 COE プログラム，第 7 回研究活動説明会資料-10，2004.

[77] 京都大学統合認証センター「IC 学生証の導入による効果」統合認証センターニュース，No.1，第 2 号，2009.

[78] 清水さや子，古谷雅理，横田賢史，櫻田武嗣 ，萩原洋一「大学における複数カードを用いた認証システムの設計」情報処理学会シンポジウムシリーズ Vol.2011,No.1,

マルチメディア,分散,協調とモバイル(DICOMO2011)シンポジウム論文集,情報処理学会,344-350，2011.

[79] 大見嘉弘「FeliCa を用いた出席管理システムの開発と運用」東京情報大学研究論集 Vol. 15 No. 2，69-81，2012.

[80] 新長章典「非接触型 IC カードと携帯電話を用いた出席管理・授業支援システム」京都学園大学経営学部論集 第 15 巻，第 3 号，1-15，2006.

[81] 大阪国パスポートプロジェクト推進委員会「大阪国パスポート　ポイントシステム「チャリ」ぽ」：http://www.osaka-pass.jp/about/charipo.html last visited September 1, 2018.

[82] PRO TECTA「SCAN LOCK RF」：http://www.pro-tecta.com/scanlock/scanlock_rf.html last visited September 1, 2018.

[83] 総合型入退室管理システム「秘堰(HISEKI)」：http://www.hitachi.co.jp/products/infrastructure/product_site/urban/security/business/hiseki/index.html last visited September 1, 2018.

[84] NFC-Diveloper.com 「FeliCa IDm とは」：http://www.orangetags.jp/words/idm last visited September 1, 2018.

[85] Sony 「FeliCa NFC の定義」：https://www.sony.co.jp/Products/felica/NFC/index.html last visited September 1, 2018.

[86] SONY：SDK for FeliCa User's Manual ver.1.24，2004.

[87] SONY "FeliCa"：http://www.sony.co.jp/Products/felica last visited September 1, 2018.

[88] APACHE：Reverse Proxy Guide：https://httpd.apache.org/docs/2.4/howto/reverse_proxy.html last visited September 1, 2018

[89] 清水さや子，戸田勝善，岡部寿男「統合 ID と属性を用いたグループの体系化」マルチメディア，分散，協調とモバイル(DICOMO2014)シンポジウム 3G-4，2014.

[90] 平岩真一「グループ管理支援システムの構築」マルチメディア通信と分散処理，No12（1993-DPS-063），pp.157-164，1994.

[91] Ananthakrishnan, R. ,Bryan, J. Chard, K. , Foster, I. more authors. Globus Nexus: An identity, profile, and group management platform for science

gateways and other collaborative science applications. Cluster Computing (CLUSTER), 2013 IEEE International Conference on, pp.1-3，2013.

[92] 柿崎淑郎，吉田啓章，辻秀一「一意なアクセスと属性間関係性の検証可能な属性情報分散管理方式」情報処理学会論文誌，Vol.51，No.2，pp.604-612，2010.

[93] 千葉昌幸，漆嶌賢二，前田陽二. 属性情報プロバイダ「安全な個人属性の活用基盤の提言」情報処理学会論文誌，Vol.47，No.3，676-685，2006.

[94] 永井孝幸，杉谷賢一，河津秀利，中野裕司「学認対応認証基盤とユーザ ID 体系移行用 CAS ゲートウェイの構築」第 11 回 CLE 研究発表会，情報処理学会研究報告，Vol.2013-CLE-11，No.20，2013.

[95] Ken Klingenstein, Kevin Morooney, Steve Olshansky. Final Report: A Workshop on Effective Approaches to Campus Research Computing Cyberinfrastructure. Document: internet2-crcc-report-200607.html, 2006.

[96] Charles F. Leonhardt. The challenges and opportunities in extending Internet2 middleware tools in medical information systems. International Congress Series, 1281(2005), pp.306–310，2005.

[97] “The Proxy Cache Engine – Open LDAP” http://www.openldap.org/doc/admin23/proxycache.html last visited September 1, 2018.

[98] Dr. Dobb's Journal “The Open LDAP Perl Backend” http://www.drdobbs.com/the-openldap-perl-backend/199102060 last visited September 1, 2018.

[99] Apache 「Apache」https://httpd.apache.org/ last visited September 1, 2018.

[100] 高倉弘喜，中村素典，江原康生，岡部寿男，宮崎修一，沢田篤史「安全なギガビットネットワークシステム KUINS.III の構成とセキュリティ対策」電子情報通信学会論文誌 B，Vol.J86−B，No.8，pp.1494-1501，2003.

[101] 大平健司，山口由紀子，八槇博史，高倉弘喜，星野寛，中野博樹「インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作」電子情報通信学会論文誌 D，J96-D(6)， pp.1483-1492，2013.

[102] 田島浩一，西村浩二，近藤徹，岸場清悟，相原怜治「ホスト登録を用いたネットワーク認証システムの実相と評価」， 学術情報処理研究，No.11，2007 .

[103] 田島浩一，近藤徹，岸場清悟，大東俊博，岩田則和，西村浩二，相原玲二，「大規模キャンパスネットワークにおける MAC アドレス認証の管理手法」学術情報処理研究，No.13，2009.

[104] 岡山聖彦，山井成良，大隅淑弘，河野圭太，藤原崇起，稗田隆「岡山大学における認証・ロケーションネットワークの構築」， 学術情報処理研究，No.15，2011.

[105] 板倉紀子，島岡章，小谷明義，吉田和幸「ユーザ機器とオンライン申請，登録，認証システムの開発とその運用について--センター管理業務の削減の観点から--」学術情報処理研究，No.16，2012.

[106] 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明「キャンパスで運用可能な MAC アドレス認証システム OpengateM」情報処理学会研究報告，2012.

[107] 大平健司，山口由紀子，八槇博史，高倉弘喜，星野寛，中野博樹「インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作」電子情報通信学会論文誌 D，J96-D(6)，pp.1483-1492，2013.

[108] 藤井邦彦，中村修，中山政勝，川上 貴教：大学等の化学物質管理システムにおけるデータベースの保守と改善点の実態調査，環境と安全 4(3) ，pp.237-246，2013.

[109] 平松綾子，一階良知， 森久博，大川剛直，薦田憲久「クライアントサーバシステム構成設計向け事例修正方式」電気学会論文誌 C，Vol.118 (1998) ， No.4，pp.592-598，1998.

[110] Cisco Systems「WLAN セキュリティに関してメリーランド大学が 発表した論文に対するシスコのコメント」2002.

発表論文一覧（2011 年以降）

1. 学位論文対象の学術論文誌

[1] 清水 さや子，戸田 勝善，横田 賢史，岡部 寿男：”統合 ID に基づく効率的な権限移譲が可能なグループ管理システム”， 情報処理学会論文誌コンシューマ・デバイス＆システム（CDS），vol.25，No.3，pp.20-31，2018.

[2] 清水 さや子，横田 賢史，三浦 悦子，萩原 知明，鈴木 直樹，吉田 次郎，戸田 勝善：”キャンパスネットワークにおけるネットワーク監視機能の運用評価と今後の展開”，学術情報処理研究，No.19，pp.3-11，2015.

[3] 清水 さや子，横田 賢史，吉田 次郎，萩原 知明，鈴木 直樹，戸田 勝善：”キャンパスネットワーク運用評価と MAC-IP 監視管理システムの構築”，学術情報処理研究，No.18，pp.53-60，2014.

[4] 清水 さや子，岡部 寿男，吉田 次郎：”一般カードを使った一時利用者向け認証システムの設計と実装”，情報処理学会論文誌コンシューマ・デバイス＆システム（CDS），Vol.3，No.1，pp.34-45，2013.

2. 学位論文対象の国内発表（査読有）

[1] 清水 さや子，戸田 勝善，岡部 寿男：”任意のグループと統合 ID を使ったメンバの管理を行うグループ管理システムの実装”，情報処理学会インターネットと運用技術シンポジウム 2013，pp.65-72，2013.

[2] 清水 さや子，岡部 寿男，戸田 勝善，吉田次郎：”一般カードを用いた認証システムにおけるハッシュ関数を用いた PIN コード生成方式”，情報処理学会インターネットと運用技術シンポジウム 2012，pp.70-77，2012.

3. 学位論文対象の国内発表（査読無）

[1] 清水 さや子，戸田 勝善，横田 賢史，岡部 寿男：”統合 ID に基づく効率的な権限移譲が可能なグループ管理システム”，情報処理学会研究報告コンシューマ・デバイス＆システム（CDS）,2018-CDS-21(29),pp.1-8，2018.

[2] 清水 さや子，横田 賢史，戸田 勝善：”グループ管理システムを用いたネットワーク管理システムの実装”，情報処理学会シンポジウム,マルチメディア,分散,協調とモバイル(DICOMO2016)シンポジウム論文集，pp.280-286，2016.

[3] 清水 さや子，戸田 勝善，岡部 寿男：”グループ管理システムにおけるグループ管理者の効率的管理”，情報処理学会インターネットと運用技術研究会，IOT28，No.18，pp.1-6，2015.

[4] 清水 さや子，戸田 勝善，岡部 寿男：”管理権限を一般ユーザにも移譲できるグループ管理システム”，情報処理学会インターネットと運用技術研究会，IOT27，No.18，pp.1-6，2014.

[5] 清水 さや子，戸田 勝善，岡部 寿男：”統合 ID と属性を用いたグループの体系化”，情報処理学会シンポジウム,マルチメディア,分散,協調とモバイル(DICOMO2014)シンポジウム論文集,pp.738-745，2014.

[6] 清水 さや子，戸田 勝善，岡部 寿男：”統合 ID 管理におけるメンバ属性を用いた拡張可能なグループ管理”，情報処理学会シンポジウム,マルチメディア,分散,協調とモバイル(DICOMO2013)シンポジウム論文集，pp.1976-1983，2013.

[7] 清水 さや子，岡部 寿男，吉田 次郎：”一般カードを使った一時利用者向け認証システムの設計と実装”，情報処理学会シンポジウム，マルチメディア,分散,協調とモバイル(DICOMO2012)シンポジウム論文集，pp.675-683，2012.

4. その他の学術論文（査読有）

[1] 清水 さや子，戸田 勝善，吉田 次郎，横田 賢史：”東京海洋大学における第 3 期 IC カード学生証導入と運用評価”，学術情報処理研究，No. 20，pp.90-96，2016.

[2] 清水 さや子，関根 卓史，吉田 次郎，戸田 勝善：”一般カードを用いた仮想 PC 教室環境の設計”，学術情報処理研究, No.17, pp.77-83, 2013.

[3] 清水 さや子，戸田 勝善，吉田次郎：”IC カード全学導入に向けた認証基盤システム整備と評価”，学術情報処理研究，No.16，pp.131-137，2012.

5. その他の国内発表等

[1] 柳沼 匠，清水 さや子，吉岡 諭，吉田 次郎：”SINET4 への移行に伴う対外接続回復の冗長化構成と評価”，学術情報処理研究，No.16，pp.125-133，2012.

[2] 清水 さや子，古谷 雅理，横田 賢史，櫻田 武嗣，萩原 洋一：”大学における複数カードを用いた認証システムの設計”，情報処理学会シンポジウム，マルチメディア,分散,協調とモバイル(DICOMO2011)シンポジウム論文集，pp.344-350．2011.

受賞

[1] 2014 年度　情報処理学会 インターネットと運用技術研究会（IOT27） 学生奨励賞受賞，「管理権限を一般ユーザにも移譲できるグループ管理システム」，2014 年 10 月.

[2] 2013 年度　情報処理学会 インターネットと運用技術シンポジウム（IOTS2013） 学生奨励賞受賞，「任意のグループと統合 ID を使ったメンバの管理を行うグループ管理システムの実装」，2013 年 12 月.

[3] 2012 年度　情報処理学会　山下記念研究賞受賞，「一般カードを用いた認証システムにおけるハッシュ関数を用いた PIN コード生成方式」，2014 年 3 月

[4] 2012 年度　情報処理学会インターネットと運用技術シンポジウム（IOTS2012） 学生奨励賞受賞，「一般カードを用いた認証システムにおけるハッシュ関数を用いた PIN コード生成方式」，2012 年 12 月.

[5] 2012 年度　情報処理学会 コンシューマ・デバイス＆システム（CDS）研究会 CDS2012 優秀論文賞受賞，「一般カードを使った一時利用者向け認証システムの設計と実装」，2013 年 9 月.

[6] 2012 年度　情報処理学会 マルチメディア,分散,協調とモバイル (DICOMO2012) 優秀論文賞受賞，「一般カードを使った一時利用者向け認証システムの設計と実装」，2012 年 8 月.